CAcert Inc., the Community CA

Security Risk Assessment

over

CAcert's Root Key

Executive Summary

Introduction

This analysis looks at the risks associated with the root key of CAcert, and especially at the need to escrow redundant copies for disaster recovery purposes.

Methodology

The analysis followed the path of ISO31000, which lays out 6 serial steps: context, identification, analysis, evaluation, and treatment. The analysis was informed by CAcert's Security Policy and many other internal documents, as well as a broader survey of current threats to similar organisations. Risks were calculated on a custom software tool developed for this purpose called *Cyclops*.

Findings

Three distinct new proposals were analysed, being escrow with a notary, m-of-n cryptographic sharing, and duplicated systems. They showed little benefit to the overall risk facing the root. This was partly because earlier mitigations had done their work, and partly because multiple copies of the root increase risk, not reduce it. The analysis was as much a battle to minimise adverse changes in risk as to benefit.

However these proposals did show different availabilities. The 3rd proposal, known as Project 5, being essentially duplicated systems, provided for both a manageable stability in direct risk to the root, and an improvement in availability.

Recommendations

It is recommended that CAcert proceeds with the proposal to duplicate the systems. In technical terms, this would create a standby system at some considerable distance, ready to start up in the event of any disaster.

New hardware would be required. A new team would have to be identified and brought in to Security Policy, and new Ceremonies established for handing over the data and keeping it current. Protection of the team and the new assets would be paramount, elsewise the risk to the root would rise.

Distribution List

1.Assessment Copy - CIT Solutions (Bruce Campus) Canberra Institute of Technology

2.Board of CAcert Inc.

3.KJE Pty Ltd Consultancy

Disclaimer

The contents of this publication reflect the opinion of the author only.

While this publication is for academic purposes, it may be taken as a guide for the initiation of a formal security risk management assessment. The author is not at the time of writing licensed as a security consultant under any state or territory law.

The quantity, quality and timeliness of information given to the author by the client will be a major factor in the thoroughness of this Assessment.

Table of Contents

1. Introduction

This Security Risk Assessment assesses the protection of the root key of a Certification Authority, CAcert Inc., and analyses several suggested techniques proposed to recover that key in times of crisis.

The root key of a CA is its primary technical asset because it signs claims that have import: protecting communications, making legal assertions and the like; any misuse of that key renders not only the entire set of existing claims at risk, but users are also vulnerable to any new forged claim. Protection of the root key is complicated because the easy method of redundancy of the root key simply raises new risks of compromise and breach. Hence, CAcert has undertaken a project, New Root Task Force (NRTF), to design a new root escrow method that meets the opposing objectives of root security and root availability.

This project has produced three leading proposals for consideration. This Assessment analyses the existing techniques and new proposals, calculates the various risk parameters over them and compares the results. While no clear winners were determined, there are enough differences to suggest a direction. In the Conclusion, this direction is expanded and explored, with some key recommendations.

This Security Risk Assessment

Two lenses are used to view the analysis. Firstly, an analysis based on ISO 31000 methodology is applied, Figure 1. Secondly, the analysis adopts a Goal of Recovery. Deriving from disaster recovery concepts, it looks at the what it takes to recover the root entirely in the event of total disaster. The golden question from disaster recovery is, if the entire fixed infrastructure (hosting, machines, team, local backups) were wiped out, what does it take to rebuild? This second lens is imposed by CAcert's audit process, and has been a long standing strategic shortfall.

Risk analysis is seen as a bottom-up methodology, and the recovery test is seen as an top-down, final-stage sanity check. Hence risk analysis will be the basis of the body of the report, and the recovery test will make more of an appearance in the conclusion.

This risk analysis proceeded along these steps:

1. establishing the context,
2. research on the input factors to identify risks,
3. programming of tools to record and analyse the risks,
4. analysis and evaluation of risks against different groupings of mitigations, and
5. recommendations for treatment.

Observations on treatment are made in the conclusion.

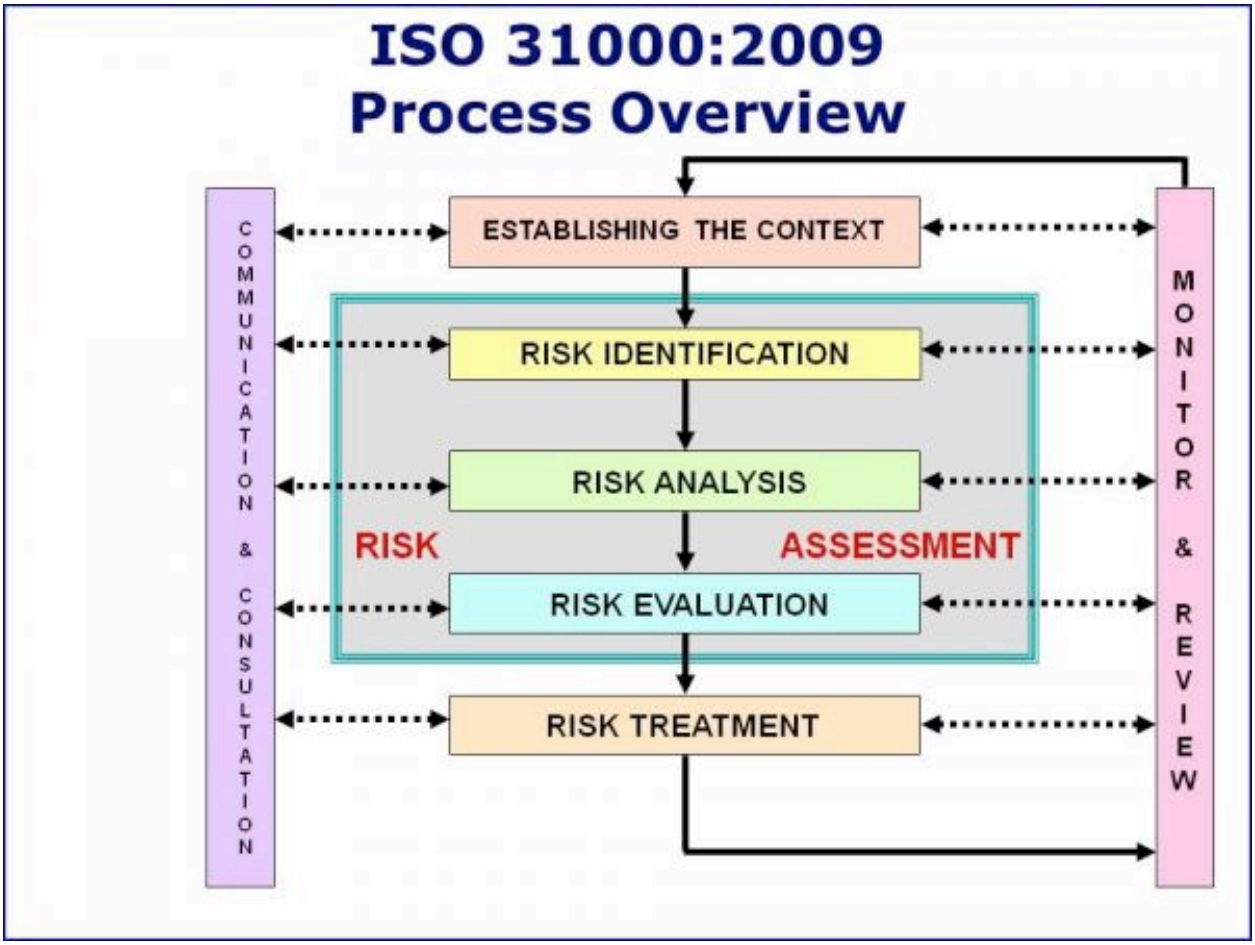

Figure 1: ISO 31000:2009 Process Overview <https://ppl.app.uq.edu.au/content/1.80.01-enterprise-risk-management>

2. The Business Context

The Business of Certificates

A Certification Authority is an issuer of *certificates*, which are digitally signed packets of digital information over a person, generally called a *subscriber*. Typically certificates can be seen as a signed statement of a person's name, their cryptographic public key, and other technical details. Binding a key to a person's name means that a secure method of communications can be bootstrapped with that person.

The interaction between the key and the certificate is analogous to that of an old fashioned lock and key. The lock is available for anyone to try their hand at, but will only accept (or verify) the right key. Less like physical keys, a cryptographic key can be used to create a signature which can be verified by the certificate. If the key is kept secret and the certificate is published, the holder of the key can be said to be able to sign claims, which others can verify but cannot forge. This signing act can be bootstrapped into a secure communication ("connection") between two parties over the Internet. The technical details are complicated and are out of scope of this assessment. Interested readers are referred to voluminous literature on Public Keys and Public Key Infrastructure, and further details are skipped over here.

Certificates find most use in online websites requiring security for e.g., taking credit card payments, online banking or other purposes where privacy and security from theft is important. In order to keep information safe, users, both merchants and customers, will want to connect securely and confidentially. This raises several requirements, including that the connection is confidential, and is connected to the right person(s). Certificates deal primarily with the latter because a certificate enables the setup of a cryptographically secure connection between named person(s). In this way, the certificate can identify a merchant to a customer for purposes of payment.

The Certification Authority - The Maker of Claims

The certificates issued to persons are signed by another certificate, being the Certification Authority's root key. In this act of signing, the CA makes a claim that the user's certificate is being held by that identified person. With this claim from a trusted provider of such claims, the holder can then go to the web and conduct ecommerce as a merchant with the general public. As ecommerce is valuable, the issuance of such claims in certificates to merchants is said to be valuable, and the CA generates quite a franchise in business if it can establish itself in this market.

In legal terms, the CA's root key signs the certificates on behalf of the Authority, thus creating a claim as part of a contract that can be tested at law.

The Registration Authority - The Checker of Claims

Making the claim in the first instance is a non-technical, non-Internet endeavour. It typically involves verifying identity documents of the user in a face-to-face meeting, and the establishing of an account relationship. This business is often outsourced to a model called Registration Authority (RA), and the CA relies on the claims presented by the RA. The CA is responsible for the creation of certificates and the security of the root; the RA is responsible for the checking and selling of claims.

Although interesting and important in its own right, the RA is generally carefully firewalled from the CA so it can be treated quite separately. For the purposes of this risk analysis, it is not relevant.

The Market for Certificates

The certificate provides an independent verification of a person, and is sold as a commercial product to that end. Typically, different CAs range from thousands to millions of certificates on issue, with pricing extending from zero to $1000. An intermediate or *subroot* can be signed and delegated by the root to sign customer certificates expressing different purposes or contracts or risk profiles; this creates a hierarchy of certificates that is transparently handled (to a greater or lesser degree) by the software.

The business of certificates is seen as potentially lucrative. Verisign, the biggest player in the industry, has twice purchased major secondary players in order to maintain its dominance of the market. The prices were indicative: Thawte was acquired in 1999 for $575 million, GeoTrust was acquired in 2006 for $125m, and in 2010, Verisign sold its CA division to Symantec for $1.28 billion (Wikipedia1). This market is hotly contested, and has given rise to the business model that might be described as: start a CA, grow rapidly, get bought out.

In curious contrast, the European market follows a different model. Domestic CAs are organised along country lines, and issue Qualified Certificates to citizens. These are even more powerful expressions of claims in certificates, being permitted by law to sign contracts up to and including in some countries wills and real estate deals. Because of the power of these certificates, these CAs are directly regulated under laws and rules. However, the market for QCs has not been successful, and even countries where QCs have been forced through via government actions and fiat, they have seen relatively little uptake and use. The implication for this risk analysis is not so much the commercial aspects but the regulatory interest hinted at in Europe.

The business also has its political ramifications. Because certificates can provide confidential communications over the net, they are also seen as doubly interesting by signals intelligence agencies such as the National Security Agency in USA and Australia's Defence Signals Directorate which generally have dual missions: *"Reveal Their Secrets – Protect Our Own"* is the mantra of the DSD (DSD). On more than infrequent occasion, the business, policies and technical details have rubbed up against national security interests, and as such, agencies are listed in the threat assessment of any CA as well as the customer list.

The Crux - The Single Point of Failure

The higher-level certificate is known variously as the root certificate, root key or simply *the root*. In practical terms, the key is kept secret and does the act of signing, while the certificate is published and does the act of verification. Something signed is said to be signed variously by the root or the certificate.

Other technical differences between key and certificate can be ignored in this discussion, what is central is that the root key has to be kept secret.

There are many fixed costs involved in operating a secure root, and typically each CA has one (or very few) root keys responsible for all claims. Generally, most CAs will now operate at least a 3-tier hierarchy: root at the top, specialist subroots signed by the root for different purposes, and user-certificates signed by the subroots (also known as end-entity certificates). Thus, risks will appear at all levels of the hierarchy, with differing characteristics.

When a user's certificate or claim is found to be in question, a revocation can be signed by the superior certificate. For example, if a user loses her key, she can request that the subroot sign a revocation over her certificate. Software is aware of this practice and will incorporate the revocation in to its calculations, thus mitigating the risk of any false proof. Similarly, if a subroot is compromised by theft or loss, it can be revoked by the root. However, the root itself cannot be revoked so easily, and thus we come to the crux of the matter: the root represents *a single point of failure* in the architecture, and the risks associated with that are very high.

The General Threat to the Root

A breach of a root key is therefore of interest to an attacker. If a copy can be made, then certificates could be issued by an attacker and various attacks -- including eavesdropping, interceptions and false statements -- could be attempted on a user's connections, leading to various harms: theft of data or intellectual property, theft of money, control of bank accounts, abuse of identity, or acquisition of other credentials. As the business of the CA is simply to sign certificates, and as the business model forces one or very few root keys, the root key becomes a singular and critical asset through which practically all the shipped product is forced, by one means or another.

Therefore it is not unreasonable to say that a root key is the CA's most important single asset, and analysis of its protection is very important.

Direct threats to the root include: unavailability of service, breach or theft of the key, loss of partners and broader reputational losses. This analysis concentrates more on the technical aspects of the protection of the root key, and places less emphasis on business aspects.

Indirect threats include the damage to the community, which includes users, partners, and many specialised workers in various roles. Although important for a CA, the issues of partners and reputation are complicated and beyond the scope of a single project, and CAcert has taken other steps to reduce the impact of risks to these assets.

CAcert's business model

CAcert differs from the above story in many interesting ways. Prime amongst them is that CAcert is a not-for-profit association that serves its members. It is not focussed on selling as many certificates as possible, and is more interested in the overall risk equation to its members. See Figure 2.

CAcert is run entirely by volunteers in their own time. People are its most important asset, but also its achilles heel: if we lose people, we cannot replace them with advertisements and money. Growth in teams and resources is slower, losses are quicker to realise.

CAcert's market is more in the low-cost, self-help area of small business, non-profits and the like. As these typically have lower risk profiles than top-drawer Internet merchants such as Amazon, the

overall risk is lower and CAcert can make different and better choices. On the other hand, differences in business model make CAcert more threatening to incumbents; to the extent CAcert succeeds, it damages others, and there is no easy pecuniary solution such as a rewarding buyout. To a large extent, this suggests that CAcert's risk profile will be distinct to that of other CAs. For this reason and others, CAcert has not been shy to steer clear of traditional industry 'best practices' and easy prescriptions.

Statistics	
User Accounts	220,887
Users with positive Assurance Points	26670
Valid Certificates	83,649
Assurers	4,939

Figure 2: CAcert Statistics, as of 15th April 2012 (CAcert stats)

3. Identification of Input Factors

In order to identify risks, it was necessary to document those factors that input into the analysis and thus contribute to the overall risk picture. For this analysis, the factors were grouped into 4 types: Assets, Agents, Scenarios and Mitigations.

Note. The term *Threat* is subject to some variability and conflation in the literature. Talbot and Jakeman tend to treat Threat as a measure of the Agent (srmbok 8.2.2 What is Threat?) whereas Joyce tends to treat it as a Hazard that has been converted into an active Threat by the presence of an Agent (KJE). That is, the scenario is the threat, the agent is more the catalyst. In this analysis I chose to treat (threat) agents and (threat) scenarios as distinct, and to treat them entirely separately in the earlier analysis, combining their effects in the later steps.

Sources

Factors were reviewed through a variety of sources. The primary internal source is CAcert's "Security Policy" (SP), the document that rules the security area of CAcert. In this sense, it establishes the set of mitigations that are arranged against the threats, but it does not list clearly the factors. An earlier input into SP was found in Philipp Gühring's "CAcert Threat Model" (Gühring), which listed many of the factors more directly. An ongoing project of the CA, the New Roots TaskForce, provided a lot of requirements and thinking, which included input from Daniel Black's "Risk Assessment" (Black). CAcert followed the David Ross Criteria, a set of audit criteria written from the relying party perspective which implied some mitigations that suggested important factors (DRC). A new report by Michael Tänzer provided an indirect lens on risks by means of documenting requirements for the software (Tänzer).

I also surveyed different mindsets in diverse security areas. This allowed selecting their headline factors, primarily for threat actors and threat scenarios. Different groups perceive different threats as being paramount, even when looking at the same general system or environment. For example, the media typically look at the lone hacker or small groups employing largely technical (and therefore scandalous) techniques. In contrast, the American privacy community focusses on governments and especially police or intelligence agencies, sometimes canonically known as the TLAs, whereas the European privacy community focusses on big business and datamining. The Certification Authority industry provides a set of documents that point at threats of concern to business objectives of CAs. The American-led military community has of late focussed on what they call the Advanced Persistent Threat (APT). Internet activists have focussed on 3rd world censorship regimes and 1st world corporations. Often the focus is driven more by what attention can be amplified through media than genuine concerns for welfare. For example, such has occurred with CNNIC (a Chinese government CA) and ichsunx2 (attacker of DigiNotar and other CAs, thought to be an Iranian government front). This tendency to scary headlines typically leaves us vulnerable to large blind spots but a survey of many competing schools can help to fill in the map.

As a sanity check, events that were documented in sufficient detail to be reliable were also recorded in A.2 History. Although not analysed, the history of attack events provides some grounding in reality for the factors selected.

Asset Identification / Resource Appreciation

Assets fall into these broad groupings: root keys for signing; hardware and hosting to protect the use of those keys and deliver the business service; teams to make it happen; a wider community of Assurers to create the basis for claims; and the large customer base that utilises the results, and enters in statements of assurance, and brand/reputation. From within these groups, more specific assets can be identified where they impact the risk analysis.

People. CAcert's members can be seen as an onion. The wider Community around CAcert numbers some 20,000 repeat users, of which nearly 5000 are Assurers (CAcert stats). Within the Assurers, around 100 have some role to play in operating the service, formed into about 10 teams. Three teams within are charged by Security Policy with protecting the *business critical assets*, being Critical System Administrators, Software Assessors and Access Engineers. Three teams provide wider governance, being the Board of CAcert Inc, the forum of Arbitration, and the policy group, and each in their way provides direction and governance to the security teams. Other teams exist and are important, but are outside scope of this risk analysis as they have no nexus to the root.

Property. Fixed assets such as hardware feature only to a small extent, and indeed the legal ownership of the hardware in critical use is vested with a partner organisation, Oophaga Foundation.

Information. The Root key is a tiny piece of mathematical data which has to be kept secret from all except for its narrow purpose, which is the signing of certificates of subscribers (by means of a cryptography algorithm called RSA). It is typically kept on a reliable and secured hardware platform, either inside a secure data centre or close by. Although it is information in the sense of data, it is treated legally as intellectual property, and thus more like fixed assets than knowledge-based information.

Roots are often seen as the major critical asset of a CA. Although CAcert does not see it 100% this way (as arguably its Community is its primary asset) it is certainly the case that the root key and surrounding infrastructure defines the set of *Business Critical Assets*.

A S S E T S	People	Property	Information	Reputation	Business Processes	Other
Teams	x					
Community	x					
Hardware		x				
root keys		x	x			
Brand				x		
Hosting					x	
Web of Trust						?

Figure 3: Assets in Groupings

Reputation. Intangible assets such as reputation or brand play less of a role than might be imagined. Typically CAcert's brand derives from several forces. Firstly, there is a strong expectation that the root key is protected and wielded in the strongest & safest circumstances, which derives from a necessary feature / flaw in the design of Public Key Infrastructure: the dependence on the root as single point of failure. Secondly, as a Community of Members rather than a profit-making business, CAcert has a compact with its users to do the right thing by them. Thirdly, industry players (CAs) have developed a marketing concept known as "*The Trust Business*," and some of the expectations implicit in that model rub off on CAcert.

For strategic reasons, CAcert has not developed its brand, preferring internal improvements before looking beyond. As CAcert Inc is a not-for-profit community of members, rather than a commercial for-profit business, it has preferred to distance itself from competitors, all of whom are commercial in nature. Further, CAcert has signed up to the concept of *full disclosure*, which is typically seen by competitors as incompatible with their view of brand development and the CA business model. CAcert is thus more relaxed about the brand than other competitors, and consequently relaxed about attacks on the reputation.

Business Processes. Hosting is similar to any website with the notable difference of needing access to the root key, or the output thereof, and the security implications of the root key as single point of failure. For this reason, the business processes of control and access over the root key, and the associated website for delivery of service, are big influences in the security model.

The technical details are strongly controlled and documented under CAcert's Security Policy (SP). In contractual terms, the ownership of assets and the contracts for hosting are handed to a local partner in Netherlands, Oophaga Foundation, which itself is a full member of the Community.

Other. CAcert often numbers its most important asset as its *Web of Trust* (or "WoT"). This is the combined graph of Members' ratings over each other for the purposes of Assurance, which generates the claims that CAcert can place in certificates. However, the WoT is carefully firewalled from the critical root area, in policies and practices. It is beyond scope of this risk analysis, but is mentioned as a contender for 'Other' assets as it is not clearly one category or another.

The full list of Assets is found at A.2 - Assets.

Agents Identification

Agents are also known as Actors, and the terms are used synonymously in this assessment. They are also sometimes known as Adversaries or Attackers, depending on the field.

Agents fall into several groupings: Competitors and near-competitors, governments and intelligence agencies, criminal groups and inside fraud, and academic and media reputational attackers. Documented attacks on CAs validate many of these attackers, see Appendix X History.

Competitors. As a competitive field, a sale from one CA is a sale lost to another. Total industry sales grow slowly and steadily, but the business is mostly a zero-sum one. In the past, takeovers either openly or by stealth have been a ploy. Recently, competitors have attempted to cartelise the SSL server-side sector by raising barriers to entry in auditing standards, and have in the past used

regulatory barriers to create defendable niches in local territories, both to some limited success. Near competitors are those that might tilt at other aspects. For example, intellectual property rights owners are well known for attacking privacy systems where there is suspicion of file sharing, and direct marketing operators are keen to acquire data on consumers.

Governments have intersected with the CA industry in two ways. Firstly, the advent of consumer-level strong cryptography on the Internet has been strongly fought, most publically by the government of USA, which attempts to preserve an advantage in international intelligence. To this end, authorities in many countries have manipulated the types and strengths of cryptography in use through export restrictions, contracts, pressure on standards organisations and other methods. The risk exists that intelligence agencies seek to breach CAs directly. A new development is the Advanced Persistent Threat or APT, which is a state-level espionage campaign against specific targets, which can involve certificates at some point in the development of the attack. In 2011, two events were claimed to be state-level attacks (see A2 - History). One CA was breached badly and subsequently filed for bankruptcy protection, and another CA lost its subroot.

Secondly, governments primarily in Europe have championed the digital signature as a way to replace manuscript or hand-written signatures, under the EU's Electronic Signature Directive (1999/93/EC). Although unsuccessful as a project, the regulatory legacy has provided an expensive barrier for national CAs, and certainly points the way to more legislative barriers.

Criminal groups concentrate primarily on spam, phishing, penetration attacks, botnets and malware of various forms in order to steal value, typically being sets of privacy data that might lead to breach of online bank accounts. They have not to date made a big impact on the CA field however this threat level appears to be on the increase. 2011 saw the first recorded criminal attacks directly involving certificates against CAs, although details are murky.

Insider attacks within CAs and where they relate to this context are typically related to random HR traumas, or attempts to insert conflicted workers into key positions. Recently a CA announced it had created and sold a subroot for the purpose of breaching employees' communications at the purchaser's business; this might be seen as an insider attack on the CA as its reputation suffered, and its privileges within vendors were threatened.

Academic and **media** as attackers are incentivised by a form of reputational gain from being named as the publisher of flaws. Academics are typically rewarded on published papers and citation counts, and media is rewarded on the level of corporate or government embarrassment that can be fed into stories, which feeds into readership and then advertising revenue. More and more, the two work together in order to cross-fertilise the credibility of their publications. Media also cover other attacks and news, where details are available. Although sometimes illegal, it is a time-honoured academic tradition to breach a system and publish the details thereof. The more blatant the breach is, the more media attention will put pressure on the organisation to respond in short order.

The full list of Agents is at A.2.

Threat Scenario Identification

Threat Scenarios are descriptions of attacks that might be undertaken by actors, each leading to consequences for the assets of the CA. As such they form a 3rd axis of investigation. In general, each scenario should be available to several attackers, and a successful result should have the same consequences regardless of which attacker triggers it as an event. Also, each scenario typically causes several consequences.

Many threat scenarios discussed in the industry and herein are theoretical, which is to say that they are un-validated by documented historical example. Only in the last few years have CAs faced sufficient direct attacks with sufficient public evidence. No pattern has formed over attacks as yet, so risk management is still more predictive than reactive.

Scenarios fall into these groups: Direct breaches of hardware and software leading to compromise, failure of service provision, governance or business issues, and reputation attacks.

Compromise. By far the most debilitating is the compromise of the root key. This can occur through failures in protection at the software, hardware, and personnel areas. Compromise includes both proven breach and uncertainty in results, and indicates not only recreation of a new root, but eventual rollout of new certificates to the users. Media attention is pretty much guaranteed to make such a compromise a survival event.

Similar effects will occur from compromise of subroots, and compromise of the systems leading to issuance of false certificates or the compromise of user data.

Failure of provision of service can sometimes be triggered by attackers, but it is also a frequent event due to non-motivated failures in software and hardware. As loss of service is common enough in the Internet world, the results are not serious if repaired within a reasonable time. An extreme case is failure of recovery methods, resulting in permanent loss of service.

Governance and business issues include loss of defect of staff, bankruptcy of the CA, loss of partners or failure of contracts, and legal suits and regulatory demands. A longer term possibility is change in laws leading to reconfiguration of business or cessation.

Reputation attacks are generally launched by academics, media, activists and unscrupulous competitors. Academic and activist attacks typically focus on the discovery of alleged flaws in protection. Generally these flaws are relatively easy to fix, but the media attention demands more of a response, and if a CA is not careful, will end up over-mitigating and introducing new risks in other areas.

The full list of Scenarios is at A.2. Note that this risk analysis also included some limited data on Hazards (which can be seen as ‘natural’ or ‘actor-free’ scenarios with consequences).

For this risk analysis, the goal of Recovery led to the Scenarios listed in Figure 3 being leading. Other Scenarios identified had only indirect impact on the root.

Scenario	Description
S.6 hard	prepared hardware snuck into system
S.7 soft	change or hack of software snuck into system
S.12 Breach K	Breach and theft of root or subroot (software)
S.17 recovery	permanent unavailability of root by recovery methods

Figure 4: Leading Threat Scenarios as directed by the Goal of Recovery

4. Threat and Consequence Analysis / Methodology

Numbers

Initially, values were estimated on a basic scheme of Low, Medium, High. In order to facilitate future-proofing of data collection and allow finer comparisons, values were collected and recorded on a range of 0 to 9, with of 1-3, 4-6, and 7-9 being Low, Medium and High, respectively. Zero is interpreted as non-present or off, a convenience for software as well as data collection.

Multiplication of Values

Combining two values to get a third in another semantic space (e.g., Likelihood X Consequences = Risk) is typically labelled as a multiplication. However this is a conceptualisation, not a mathematically rigourous transform. In practice, the combination of two values is more of a nuanced operation. This risk analysis used several methods, including tables and mathematical formulas, some of which are displayed in tabular form in Annexes 3, 4. In switching between different methods, no significant impact on results was observed.

Factor Analyses

Agents. For each Agent, values were estimated for each of Resources, Knowledge, Confidence, and Desire. Resources and Knowledge were multiplied (as described above) to get Capability, and Confidence and Desire were multiplied to get Intent. These latter results, Capability and Intent were multiplied to get 'Threat' (srmbok 8.2.2).

Assets. For each Asset, values were estimated for each of Recognisability, Exposure, Accessibility. These three were multiplied together to give Opportunity. In addition, each asset was rated as a Business Critical Asset according to Security Policy, and given a criticality rating that reflected its essentiality to the business and its capability for loss to bring the business down (1 to 9 with 9 being high).

Scenarios. For each Scenario, values were estimated for each of Suitability, Accessibility and Deployability. These three were multiplied to give Effectiveness.

Mitigations. For each Mitigation, the Principal (initial) and Annual costs were estimated.

Cross-Factor Values. Between the Factors there are matrices to determine the strength of the connection.

Connection	Factor 1	Factor 2	Description
Attractiveness	Agent	Scenario	How attractive the Agent finds the Scenario
Vulnerability	Asset	Scenario	How damaging the Scenario is to the Asset
Opportunity	Mitigation	Asset	How much the Mitigation protects the Asset, by for example reducing the Opportunity
Effectiveness	Mitigation	Scenario	How effective the Mitigation is against the overall Scenario

Figure 5: Cross-Factor Values

Derivative Risk Analysis

Risk is calculated as Likelihood multiplied by Consequences (A3-1). Both of these values are estimates over a particular Scenario.

Likelihood. To calculate the Likelihood of a Scenario, this has to consider Likelihood of each Agent to attack using that one Scenario, and combine them into one overall likelihood of the Scenario eventuating from any attacker. Each Agent's Likelihood against a Scenario is calculated as the Threat multiplied by an Attractiveness (a cross-factor Agent-Scenario value).

Agent's Threats in turn are calculated as Intent multiplied with Capability (A3-2). Intent is calculated as Desire multiplied by Confidence (A3-3), and Capability is Resources by Knowledge (A3-4).

In combining the Likelihoods of all Agents, we have to take into consideration that Likelihood is on a logarithmic scale. A low Likelihood might be 1 in 10 years; whereas a high Likelihood might be 1 per month. Combining these together should result in 1 per month. In order to approximate this, each individual calculation of an Agent's Likelihood is raised to a power (at the time of writing *e*) then summed and then logged back (using log-base-*e*). An alternate simpler approximation is to take the largest Likelihood and use that as the proxy result for all Agents.

For net present value purposes, Likelihood was placed on the logarithmic scale in Figure 5. In the calculations, a simple formula was used (10 / 3.2 ^ (9 - Likelihood)) to calculate events per annum, and the result of this was directly multiplied by the dollar value of costs to give expected value of any event(s).

Likelihood	Elapsed Time per Event	Events (Chance) per year
1	1000 years	0.001
2	320 years	0.0032
3	100 years	0.01
4	32 years	0.032
5	10 years	0.1
6	3.2 years	0.32
7	1 year	1
8	4 months	3.2
9	5 weeks	10

Figure 6: Likelihood expressed as Time per Event, or Chance per Year, for Financial calculations

Consequences. In similar fashion, Consequences of a Scenario are calculated over all Assets. For each Asset, the Consequences are calculated as the Asset Consequences multiplied by Opportunity, Vulnerability and the Scenario Effectiveness. This calculation is further multiplied for *business critical assets*. Then, for the Scenario, all Asset Consequences are summed in a logarithmic fashion as above.

Risk. Finally, Risk is calculated as Likelihood by Consequence, for each Scenario. See A3-1.

Mitigations

Mitigations effect many aspects, mostly on the Scenarios and Assets. Mitigations typically do not change the Agent's situation, but they can reduce the Effectiveness of Scenarios and the Opportunity of Assets. Therefore 2 matrices record those values: for each Mitigation, the change in Effectiveness and the change in Opportunity. The change can be recorded as either a positive or negative effect.

Programming

With the size of the CA root key risk project, it became clear early on that the degree of depth required and number of factors involved would result in an explosion of calculation, which would be lost any time the base numbers change. That is, re-working the calculations would be tedious and impractical. Therefore a programmed system of some form was indicated.

The system was coded up within an existing web application framework, and is referred to by its working codename of *Cyclops*, a play on "in the land of the blind, the one eyed man is king." The system stores the variables described above for each of the factors, and analyses the Risk dynamically. This allows fairly convenient *what if* analysis. Lessons drawn from the experience of building the system are included in Appendix 6, Wider Observations on Methodology.

Raw statistics: the system is written in object-oriented PHP, as part of a web-application supporting several management tools for open source and CAs. *Cyclops* has at time of writing 5000 lines of code (5 kilo-lines-of-code or kloc) and the wider system has 20 kloc inclusive of *Cyclops*. It presents a dozen screens, of which half are display only, half are for inputting data. All results are calculated on the fly, dynamically, and displayed on demand. The graphics in Annexes 2, 3, 4 are screen shots taken from the display screens.

5. Security Risk Management Techniques

Mitigations were surveyed in much the same way as earlier factors. Existing mitigations are relatively well documented within the Security Policy process. There is a long-standing project to develop a new set of roots, which has proposed three new strategies including new mitigations. These became the basis of the risk analysis.

Grouping of Mitigations into Projects

Mitigations or techniques can be divided conceptually into several sets which for this section only I will label as conceptual groups (a) through (d). Existing mitigations can be seen as (a) those that are ordinarily expected in any mildly secure operation, (b) those that are already in place to raise the bar to a perceived high security needed for CAs, and (c) those that are already selected but are not as yet in place. To which we can add (d) proposed mitigations, found out of the set proposed by CAcert's New Roots Task Force.

Group	Project	Definition	Examples
(a)	0	Ordinary mitigations expected in any website	Passwords, etc. These are not examined or listed further.
(b)	1	High security mitigations in place for CA operation	Dual control, full disk encryption
(c)	2	New mitigations chosen but not as yet in place	offline root
(d)	3-6	Mitigations that are proposed but not as yet selected	New Roots Task Force

Figure 7: Mitigation Projects

The risk analysis system, *Cyclops,* takes groupings of mitigations in Projects. From the above, group (a), ordinary mitigations, is called Project 0, as the *null selection*. Within Project 0, any mitigations are ignored completely in this analysis, although audit and other reviews can be expected to cover them. For example, common issues such as password strength, handover processes, contracts, and so forth are assumed.

Group (b), mitigations already in place for high security needs, is labelled Project 1. Group (c), mitigations already selected but not in place, is labelled Project 2. Beyond those, there are various proposals that have not been accepted, and these are labelled Projects 3 through 6.

From here on we will use the Projects metaphor and dispense with the "groupings".

Adequacy of Existing Security Risk Management Strategies - Project 1

As the primary asset demanding clear protection, CAcert's root is well protected at least to an ordinary business level. Security Policy has imposed dual control over access to the root for non-routine signing, and a very small team of vetted individuals can participate in that protocol. The transfer into a high security facility has helped a lot. Two independent encryption layers protect the root from static attack.

Weaknesses exist, and some of these have contributed to a result of *audit fail* in an earlier review by this author. Firstly, the root is online, as it is an active signing root. This raises the possibility that false certificates including subroots can be issued via hacking, and also that the key itself may be leaked by weaknesses in the protection regime. Secondly, the regime provides for only one working copy, and there is no independent recovery strategy in place. Although there are backups, their recovery status is unknown.

The primary cause of the *audit fail* over the roots themselves was the lack of any documented history over protection prior to 2007, which has been addressed in principle by the decision to create new roots. This process is pending the design of a suitable root escrow method to meet requirements for recovery, analysing which forms the objective of this report.

Adequacy of Accepted Additional Mitigations - Project 2

The major additional protection already accepted is for the root to be offline. This addresses the risks of unauthorised subroot signing and root leakage via hacking. It also mitigates against static (data center) attacks as a live online root would be presumably available ins some form at some digital level.

Analysis of Proposed Security Risk Management Strategies

What remains to be proposed is a method of root escrow that supports a complete recovery exercise. In this scenario, the existing setup is wiped out, and the CA must reach back to primary backups, new teams, new hosting and new hardware. Hence the primary goal of this risk analysis is to recommend a strategy for key storage against the recovery requirement.

Three proposals were considered, shown in Table 6.

Project	Description	Mitigations
3 (NRTF-P3)	remove the root out of the data center and protect it elsewhere inside an independent team. This proposal is expected to split the key using an m-of-n cryptographic scheme.	split key (M.6) taken out of data center and held by independent team (M.10) protected using m-of-n cryptographic scheme(M.11)
4 (NRTF-P4)	Place a copy of the root into escrow with a Notary or similar, and a copy in hosted center under control of critical team.	place unattended copies in HSM (M.4), escrow one copy with Notary (M.3), create recovery backup on regular basis (M.13)
5 (NRTF-P5)	Duplicate the signing server and escrow the duplicate with a foreign team.	duplicate signing server (M.16) and place keys in HSMs (M.4)

Figure 8: New Mitigations in Projects 3-5

These projects were entered in to the risk analysis tool for comparison with the three earlier ones.

Each Project showed quite mild effects over-all. Although the mitigations identified were quite strong in themselves, they had to compete for efficacy against existing mitigations -- positive effects were quite subtle in comparison.

Further, as much as they might by themselves improve the overall risks, the goal of Recovery goal interfered. Recovery by its nature now emerged as something that increased risks according to the model, partly because recovery requires multiple copies of the root, and partly because recovery assumes that disaster has already happened, which means higher risks are more acceptable than before disaster.

No project was able to reduce the risk of key breach (via scenarios S.6, S.7, S.12), an important and hoped-for outcome. On careful review of the data and analysis, several factors: (a) much hard work had already been done with existing mitigations, and there are no low hanging fruit; (c) recovery by its nature assumes destruction of assets, and the consequent need for spare copies of assets - which automatically increase risks by duplication; and finally (c) the overall risk had been moved from High to Moderate, and the nature of the application and its dependence on a *single point of failure* in the root key seems to resist pushing risk further down to Low. This stubbornness does not appear unreasonable given the overall risk profile of the Certification Authority. Instead, modelling and analysis became a battle of minimising the increase in risks to S.6, S.7, S.12 as much as reducing them.

Where the projects did differ is that they had differing effects on Key Availability, an important but opposing requirement of the CA. In this case, they are almost clear opposites of interest: as Availability goes up, risk of Leakage goes up as well.

Project 3 (NRTF-P3) demonstrated a dramatic increase in the risk of failed availability, taking it from Low to Moderate. This project creates a single copy and escrows it within a team using cryptographic methods to spread the copy across the team. Typically this method is called *m-of-n*, as it requires the bringing together of a sufficient quorum *m* of a total of *n* team members in order to recover the secret. However this technically delicate method brings risks of its own as there is the possibility of the exotic techniques themselves getting in the way.

Projects 4 and 5 demonstrate none of this eccentricity. They both simply duplicate the key, and then see to protecting it. The difference is in their use of protection. Project 4 (NRTF-P4) escrows a key with a (European) Notary, being a trusted person who makes their entire reputation on the basis of protecting assets such as real estate and wills of last testament to the strongest extent possible. Project 5 (NRTF-P5) places a copy in a spare server, and stores that with an independent team (or context). The duplicated server, because it is more of an answer to a complete recovery exercise, providers better availability, and thus lowers the overall risk without unduly increasing risk of root compromise.

Recommendations

The different proposals all had similar effects on the risk of Key Compromise - minimal, unmeasurable or adverse. However they varied in their effect on Key Availability. As the Recovery Goal was a strong input into the risk analysis, it is a sufficient foundation on which to base a recommendation

Project 3 was eccentric. Because the Project splits the root amongst a diversified team, it reduces recovery prospects and therefore is not recommended.

Projects 4 and 5 did not impact recovery in the numbers. They differ in that Project 4 places a safe copy of the root with an external party such as a European-style Notary, whereas Project 5 creates a second system and duplicates the availability internally.

Although this was not well-reflected in the risk calculations, Project 5 is the clear winner in recovery terms because it protects so much more than just the root key. In short, it opens the way to a fully recoverable system for all sorts of disasters, not just ones effecting the roots.

New System in Standby for Disaster Recovery

Therefore Project 5 is recommended, being the creation of a new duplicated system, to be held in stand-by, and to be escrowed under the care of a separate team. Initially this should be the signing server as identified in M.16, but should be expanded in time to cover the full service suite.

However this recommendation is tenuous - it goes beyond the ambit of the risk analysis as originally conceived. This extension is because the recommendation for Project 5 and a duplicated system and team will have much wider ramifications for the structure, culture, and people of the CA. Indeed, it will likely be controversial and require much debate and hard thinking.

Therefore this risk analysis stops short of a prescriptive Risk Treatment Schedule & Plan. Instead, the prototype in Figure 8 is offered to provide the scope of the problem. It is but one way forward, and will no doubt be adjusted when the dust settles on the larger question of accepting the recommendation for Project 5.

Mitig'n	Task Description (augmented)	Responsibility	When	Who
M.4 HSM	put root onto HSMs (all copies) - review popular devices, trial a couple for usability, select and build ceremony.	Software Assessment Team Leader	over a period of year	Software Assessment with support from Critical Systems Team
M.5 offline	take root offline so cannot be accessed without human intervention, not wired at all - investigate low-cost methods to separate root from sub-roots, and power down the former.	Critical Systems Team Leader	Final step, only to be done when M.4 and M. 16 complete.	Critical Systems Team - Ede group.
M.20 (new)	*create new Recovery Team to (a) secure hardware for signing server, (b)coordinate with Critical Systems Team in conducting Ceremony, (c) negotiate on-demand hosting, and (d) conduct disaster recovery process. This task will involve canvassing the existing regional and country communities for possibilities.*	Board	over a period of a year	All strong country and regional communities invited to participate
M.16 dup-ss	duplicate / backup the signing server (ss) and secure the backup ss in another location	Recovery Team Leader	when M.20 complete	Recovery Team with assistance from Critical Systems Team
M.21 (new)	*Repeat above M.20+M.16 process with the main webserver and database*	Recovery Team Leader	when M.16 complete	Recovery Team with assistance from Critical Systems Team

Figure 9 - Risk Treatment Schedule & Plan - Prototype only

Conclusions

This risk analysis looked at methods for protecting the CA's root, and how best to improve the availability in the event of disaster. As this is a project with some maturity and a fairly clear and understood risk of attack, most of the mitigations needed were already in place. Hence newer mitigations had trouble effecting the overall ratings.

However, a difference was found in availability. This was surprising to this reviewer. What the risk analysis is saying is that in effect, improving the protection is hard, but improving the availability is still possible. Each of the mitigation projects proposed had quite substantial costs attached to them, so recommending them without some showing in improvement is hard.

The narrow recommendation of creating a duplicated system is easy to say. To implement is quite substantial: if CAcert were to accept this recommendation in its fuller guise, it would need to create a new team, investigate new hosting possibilities (if not contract them) and secure new hardware.

Events (ceremonies) for duplication would be needed, and protocols for disaster recovery should be put in place. Most importantly, the risk of compromise via the new team must be closely watched.

However, this proposal has the singular and spectacular advantage of meeting the wider need for a complete disaster recovery plan. To date this has not been handled well by the organisation, and the consequences of this lack have played their part in the poor showing in the earlier audit review.

Recovery - the precise Goal of this analysis - increases risk. The chosen project does the least damage to risks, as opposed to the more expected overall reductions expected by such close attention. Having said that, a recovery plan is an audit and strategic necessity of the business. We have to wear that cost.

Annex 1 - Terms of Reference

TERMS OF REFERENCE ANNEX 1

Annex (1)
Canberra ACT
SRA date: 2 March 2012

Security Risk Assessment

Introduction
This Security Risk Assessment (SRA) venue was allocated by instructor Keith Joyce as the final assessment item for the Diploma of Security and Risk Management, run by Australian Security Education & Consulting Pty Ltd, a Canberra-based training organisation (ASEC) and CIT Solutions, a division of Canberra Institute of Technology.

The consultant, Ian Grigg, developed the Terms of Reference (TOR) in consultation with the client, CAcert Inc, as represented by President Lambert Hofstra on 31st of January, 2011.

The SRA will cover the root key project of CAcert. This TOR, as agreed to by the undersigned, will determine the conduct and extent of the SRA regarding the root asset. This TOR will be included in the SRA's Report.

Contents

The contents of the TOR are as follows:
Objectives
Authority
Scope and nature of the SRA
  Inclusions
  Exclusions
Information Sources
Methodology
Benchmark
Resources
Outcomes
Assumptions
Cost/ Timeframes
Implementation
Confidentiality and Publication

Context

CAcert runs as part of its suite of services a Certification Authority or CA. This service signs "certificates" for end-users with a root key. As the user-certificates make claims of legal import, leading to risks, liabilities and obligations, the root key must be kept secure in relation to those costs. The root key of a CA is typically created, stored and utilised in an environment of a high level of security.

Objectives

The objective of the SRA is to analyse and report on the security of CAcert's root protection system and process (in short, the root).

The TOR details the agreed-to guidelines for the client and consultant in regard to the execution of the SRA. Consequently the SRA will be conducted as outlined in this TOR with the exception of any subsequent and mutually agreed to amendments. All amendments are to be in writing (email).

The SRA will be conducted over 2011 and the Report delivered to ASEC for assessment in early 2012. After assessment, the Report will be formally delivered to CAcert Inc.

Authority

The client authorises the consultant to conduct the SRA of the root, as outlined in the TOR.

The board's motion m20120127.2 is the authority for this TOR for the consultant to conduct the SRA as stipulated in the TOR.

Scope and Nature of the Security Risk Assessment

Inclusions

The following areas/ issues are to be examined as part of the SRA:

Personal security and safety of critical personnel engaged in creation, protection and usage of the asset.
General security of critical personnel and participants working remotely.
Physical security of the root - Premises, devices and safes.
Physical security of online information technology hardware and software.
Information technology infrastructure (see exclusions for limitations).
Factors affecting the reputation of the CA.
Factors affecting the business of the CA.
Compliance with applicable legislation (safety, contractual) in regard to the activities.
Compliance with applicable policies and procedures.
Security procedures during creation, protection and recovery.
Security response by the critical personnel.
General business policies and procedures affecting the asset.

Exclusions The following areas/ issues will be excluded from the SRA:

Computing areas outside Ede and the creation/recovery facility.
In-depth examination of the computer server room.
General integrity of computing infrastructure.
Incident Reports – if any.
Arbitration Rulings – if any.
Testing of emergency response in Ede.
Qualifications and insurances held by critical personnel
Adequacy of business-layer defences, e.g., insurance.

Information Sources

The client will provide:

Policies and procedures for root asset critical protection.
Authority to obtain other information, if necessary, from critical personnel.
Introduction and authority to approach critical personnel.
Authority to approach the external security contractors (Oophaga).
Access to, or obtaining the following information sources (if deemed necessary by the consultant) will be the responsibility of the consultant.

Digital Signature Directive
Electronic Transactions Act (various)
Privacy Act (1988)
Arbitration Act (various)
OHS legislation (various)

The consultant is authorised to conduct interviews with all current members of management and staff. However the consultant will notify the client before contacts are made outside CAcert. All interviews will be conducted using the normal Internet communications methods of CAcert.

All information obtained by the consultant for the SRA will be by legal means and once obtained, protected according to CAcert's Security Policy and related policies and practices. Consultant is to determine that information which requires especial care (m20120127.1).

Methodology

The consultant will use the following methodology to carry out the SRA:
Research – identification of key areas in relation to the root asset.
Discussions with the client.
Discussions with critical staff.
Formal agreement to the TOR.
Site Inspections.
Discussions with CAcert Executive (board), as necessary.
Procurement and examination of Practices and similar written material.

Compilation of the SRA Report – this will include a Risk Register, Risk Treatment Plan, and a list of all written material referred to.

In regard to the above, reliance will be made on previous work where possible.

In regard to risk analysis for the SRA the consultant will use the ISO 31000:2009 /Australian/New Zealand Standard 4360:2004 – Risk Management (AS/NZS 4360:2004).

Benchmark for Risk

The benchmark level of risk set for the SRA was determined in consultation with the client. This level is Medium.

The Risk Register will include assets identified and the risk to them. However, assets subsequently analysed with a level of risk below the determined benchmark will not normally be considered or form a part of the final report and recommendations. The Risk Treatment Schedule and Plan will only address treatments for risks identified to those assets at or above the benchmark, unless otherwise specified.

Resources

The client agrees to provide the consultant with the following resources for the SRA:

- Printing costs
- Graphics

Agreed limit: $100. The consultant will provide all other resources – however:

Extra-ordinary resources: If it becomes apparent that during the SRA extra-ordinary resources are necessary, the supply of these resources by the client is to be by mutual agreement between the client and consultant.

Outcomes

The consultant will produce a comprehensive written Report of Findings for assessment by May 2012, unless varied in writing by mutual agreement by the client and the consultant.

The Report of Findings will include a complete Risk Register and Risk Treatment Schedule and Plan for CAcert using the ISO 31000 and AS/NZS 4360:2004 Risk Management formats. These details are to be provided as annexes to the Report.

The consultant undertakes to notify the client of any risks, if identified, which require immediate attention. It is at the sole discretion of the consultant to report other areas of concern prior to the final Report of Findings.

The recommendation of the SRA report will comply with applicable legislative and policy requirements. Any inconsistencies between the SRA Report and the organisational management policies and procedures of the Critical Teams may be detailed in the SRA.

Assumptions

The consultant is not required to travel, unless by mutual agreement between the client and the consultant.

Expenses that are not detailed in the *Cost* section of the TOR are to be approved by the client.

The client undertakes to inform, or provide a reference point, to all personnel who may be involved during the SRA the responsibilities and reason for the SRA.

Cost/ Timeframes

There will be no retainers levied for the SRA of the Root since the purpose of the SRA is for course assessment. The client agrees to the following limited & basic costs.

Printing costs
Graphics

Agreed limit: $100. The client and consultant will agree to any changes in costs that arise because of mutually agreed to changes in the TOR.

Consultant will rely on information from prior work, especially prior visits to Ede, NL to the extent possible. If necessary, subsequent visits may be arranged on mutual agreement. During this period the consultant will be given negotiated access to the critical personnel during normal working hours (9am to 5pm).

The SRA will be conducted throughout 2011. The consultant will be given negotiated access to the critical team.

Confidentiality and Publication

Confidentiality is preserved under CAcert's normal policies and practices.

The Security Risk Assessment Report is classified as an open input to Security Policy. The Consultant is responsible for advising of any sensitive data before publication (m20120127.1).

Note: For the purpose of course assessment CAcert is advised that another person is involved.

That person is:
Keith Joyce – Risk Management Trainer, ASEC / KJE.

Terms of Reference agreed by:

Piers	*Ian*
.....	.....
Piers Lauder (President, CAcert)	Ian Grigg (Consultant)
Date: *07* / *03* / 2012	Date: *7th* / *march* / 2012

Annex 2 - Input Factors

A2.1 - Assets Register

Idx	Name	Description of Agents (10)	D	C	R	K
A.1	APT	Advanced Persistent Threat (APT) is synonymous with State or military intelligence agency (TLAs) operating extra-legal. Capable of long term, multi-victim attacks for specific assets of high value, e.g. RSA/Lockheed Martin	4	6	7	7
A.2	RBN	private organised crime organisation	3	8	5	6
A.3	Law	DoJ/State Department/Foreign Ministry, pursuing legal means	2	3	4	3
A.4	Comp	Direct Competitor in space, such as another CA	3	5	4	7
A.5	Interested	Interested party or near-Competitor in similar space, such as Intellectual Property Enforcement Agency	7	4	7	3
A.6	Insider	Someone working within the organisation - fraud, vandalism, spite, extortion	5	7	3	5
A.7	Partner	A supplier of some component or service	1	3	5	6
A.8	Cracker	Lone criminal	5	7	3	7
A.9	Uni	Academic researcher	7	3	3	6
A.10	Press	Journalists, Media Publisher, Blogosphere, Paparazzi security press	9	5	2	2

Glossary: **D**esirability, **C**onfidence, **R**esources, **K**nowledge.

A2.2 - Threat Actors

Idx	Name	Description of Agents (10)	D	C	R	K
A.1	APT	Advanced Persistent Threat (APT) is synonymous with State or military intelligence agency (TLAs) operating extra-legal. Capable of long term, multi-victim attacks for specific assets of high value, e.g. RSA/Lockheed Martin	4	6	7	7
A.2	RBN	private organised crime organisation	3	8	5	6
A.3	Law	DoJ/State Department/Foreign Ministry, pursuing legal means	2	3	4	3
A.4	Comp	Direct Competitor in space, such as another CA	3	5	4	7
A.5	Interested	Interested party or near-Competitor in similar space, such as Intellectual Property Enforcement Agency	7	4	7	3
A.6	Insider	Someone working within the organisation - fraud, vandalism, spite, extortion	5	7	3	5
A.7	Partner	A supplier of some component or service	1	3	5	6
A.8	Cracker	Lone criminal	5	7	3	7
A.9	Uni	Academic researcher	7	3	3	6
A.10	Press	Journalists, Media Publisher, Blogosphere, Paparazzi security press	9	5	2	2

Glossary: **D**esirability, **C**onfidence, **R**esources, **K**nowledge.

A2.3 - Threat Scenarios

Idx	Name	Description of Scenarios (17)	V	C	A	H	S	A	D	E
S.1	contract	breach of contract	4	4	9	3	4	3	1	3
S.2	walk	disappearance of key person or partner.	7	7	8	8	7	5	7	6
S.3	defect	change of loyalty of key person or partner.	8	9	7	5	6	5	5	5
S.4	bankrupt	closing of the business through financial failure.	3	5	5	3	2	4	6	4
S.5	legal	legal attack on key person, partner or self.	5	5	3	2	5	5	4	5
S.6	hard	prepared hardware snuck into system	7	8	9	8	8	8	7	8
S.7	soft	change or hack of software snuck into system	7	9	5	8	9	7	8	8
S.8	rep	deliberate reputational attack, including false breach claim	5	3	5	5	2	8	6	5
S.9	FUD	Published noise on vague security basis such as Numerology	3	2	5	8	2	6	7	5
S.10	Theft	Theft of important hardware	8	7	5	3	6	3	2	4
S.11	BreachD	Breach and theft of personal data or certs via website	8	7	5	9	6	7	7	7
S.12	BreachK	Breach and theft of root or subroot (software)	6	9	5	5	9	4	4	6
S.13	Crypto	Weakness exploited in Cryptography or Algorithm to reveal key data: PKI, TLS, x509, RSA, SHA1, SHA2, MD5	3	8	1	4	3	1	8	4
S.14	law	Change in law / legislation effecting legality of business, opening up liabilities, or imposing traumatic barriers or conditions to privacy and security. Sometimes known as country risk.	3	6	5	4	4	3	5	4
S.15	fail	failure of hardware, software, crypto into a non-operable position leading to temporary loss of service of main business services (not root)	6	5	4	2	3	7	5	5
S.16	keys	temporary unavailability of root for signing (CRLs, OCSP keys, new subroots)	6	5	5	5	5	3	2	3
S.17	recovery	permanent unavailability of root by recovery methods	9	9	5	4	7	7	5	6

Glossary: **V**ulnerability, **C**onsequences, **A**ttractiveness, **H**istory, **S**uitability, **A**ccessibility, **D**eployability, **E**ffectiveness.

A2.4 - Mitigations

Idx	Name	Description of Mitigations (19)	S	P	A
M.1	dual control	it requires two (or more) persons to access root, including 4 eyes	D	500	10000
M.2	FDE	full disk encryption in software (kernel) or equivalent for token copies (e.g., dual encryption on tokens to reduce consequence of loss)	D	1000	200
M.3	escrow-TTP	place a copy of root with an external TTP (with European Notary or in bank vault) independent of other copies	P	3000	500
M.4	HSM	put root onto HSMs (all copies)	Y	10000	5000
M.5	offline	take root offline so cannot be accessed without human intervention, not wired at all	Y	5000	2000
M.6	split	split the root between two (or more) assurers outside the critical team to create a dual control mechanism (no redundancy)	P	500	500
M.7	hisec-host	secure the signing server and business server in a high security facility	D	10000	2500
M.8	soft	Software Assessment controls as per SP7	D	10000	3000
M.9	audit	review over all documentation, comparison with practices, imposition of some practices.	D	100000	100000
M.10	indie root	take root out of data center (removes data center copy, independent of other copies, so other copies must be added somewhere)	P	3000	5000
M.11	split-n-of-m	split the root between N * Key Holders and M * Key Guardians using OpenPGP	P	2000	2000
M.12	split-pw	encrypt the root between P1 group (N Members) and P2 group (M Members) using OpenSSL encrypt of key (leave encrypted root on signing server)	P	2000	2000
M.13	backups	encrypt the root into a backup prepared annually at AGM time (leave accessible root on signing server)	P	0	500
M.14	split-TTPs	encrypt the root into a USB for escrow to one TTP, put password in escrow with another TTP; extra coverage with 3rd and 4th TTPs	P	1000	600
M.15	split-SSSS	encrypt the root into a USB; use SSSS to create N shares of the passphrase, distribute the shares to N Key Guardians	P	2000	2000
M.16	dup-ss	duplicate / backup the signing server (ss) and secure the backup ss in another location	Y	4000	2000
M.17	ceremony	Root key creation and signing ceremony (including subkeys) as per SP9.2	D	5000	5000
M.18	Arb	Exceptions processing is referred to Arbitration as a dispute	D	1000	5000
M.19	Redundancy	The principle of redundancy requires teams to have more than enough people	D	0	5000

Glossary: **S**tatus: one of D - Deployed, A - Assumed, P - proposed, Y - accepted, 0 - no decision, what if?, *(empty)* - unset?
Status: one of **D**eployed, **P**roposed, **acc**cepted, **A**ssumed, '0' what-if.
Principal is the initial cost of project, **A**nnual is the yearly cost of maintenance.

A2.5 - History - Documented and Validated Attacks

Only attacks validated by reports are listed here (History). To some extent, where we set the bar is difficult to justify because we lack a clear history of user damages. However, some history is better than none. The **primary source** for this document is located at http://wiki.cacert.org/Risk/History ; a more up-to-date version and references can be sourced through that page.

2001. False certs. An unknown party used weaknesses in validation to get two certificates issued in the name of Microsoft.com (Guerin). The attacker was thought to be of the reputational variety: interested in embarrassment of CA not exploitation.

2003. Phishing. This attack bypasses the security afforded by certificates due to weaknesses in the secure browsing model (Grigg1). The existence of an unsecured mode of communication (HTTP) alongside a secure mode (HTTPS) provides an easy borders-of-the-map or downgrade attack, which user interfaces offer little resistance against. Consequences best guesstimate runs at around $100m per annum (FC 1343).

2008. Interface breach. One CA created a false certificate for a vendor by probing the RA of a competitor for weaknesses (Leyden). Consequences limited to lowered reputations for all of those involved.

2008. Weak root. An academic group succeeded in attacking a CA with weak cryptographic protections in its certificates (Sotirov et al). This resulted in the attackers acquiring a signed certificate over two keys, one normal and one that acted as a sub-root. This gave them the ability to sign new certificates that would be accepted by major vendors. Consequences: as the root that was attacked was slated to be removed within the month, consequences were limited. Faster rollout of the new root, perhaps a few certificate re-issuances and reputation damage.

2010. Stuxnet. Two code-signing certificates, stolen from two separate chip manufacturers in Taiwan, were used to sign drivers that were installed as part of a rootkit to infect Windows machines (Krebs), (Wikipedia1). The overall goal was a highly targetted sabotage of Iranian centrifuges engaged in production of high-grade nuclear material. Consequences: Various non-authoritive reports suggested that Stuxnet succeeded in knocking out and perhaps destroying some 1000 centrifuges, estimated at 10% of Iran's centrifuge capacity (ISIS). DEBKA suggests the damage is far more severe and sweeping than first reported, effecting and targetting thousands or even millions of significant computers (DEBKA1), and carrying on into 2012 (DEBKA2).

2011. False certs. A lone Iranian attacker, ichsunx2, breached approximately 4 CAs. His best success was to use weaknesses in an Registration Authority to acquire 9 certificates for several high profile communications sites (Zetter). It was claimed that the attacker operated under the umbrella of the Iranian state but no evidence for that was forthcoming.

2011. Breached / collapsed CA. The same attacker, icksunx2, breached a Dutch CA and issued several certificates. The CA's false certs were first discovered in an attack on Google's gmail service, suggested to be directed against political activists opposed to the Iran government. Controls within the CA were shown to be grossly weak in a report by an independent security auditor (FOX-IT1), and

the CA filed for bankrupcy protection (perhaps for that reason). Vendors discovered that revocation was not an option, and issued new browsers that blocked the CA in code. Known user damages: rework by google, and vendor-coordinated re-issuance of software to all browser users. Potential for loss of confidentiality of activists opposed to Iranian government. Many Netherlands government agencies had to replace their certificates.

2011. Certificate Stealing. 3 separate incidents indicate that certificates are now worth stealing. Infostealer.Nimkey is a malware distributed through traditional spam/phishing channels (Yahoo). Once it infects, it searches the victim computer for keys and sends them to a server in China. Duqu is a variant of Stuxnet that used a stolen code-signing cert to install drivers (Wikipedia2). From inspection of the malware, the attack was variously quoted as IP/data collection/espionage, stealing keys, or attacking CAs (McAfee). Identity fraud of some form was used to get a valid certificate issued in the name of a company by intercepting the verification communications to that company's employee (F-secure). Consequences. Re-issuance of certificates and reviews of security. In none of these 3 cases were any direct damages assessed.

2011. Spear Phishing. A group of 9 certificates were identified in targetted malware injection attacks (FOX-IT2). As the certificates were all alleged to be only 512 bits, the conjecture is that new private keys were crunched for them. One public-facing sub-CA in Malaysia was dropped, 3 other CAs re-issued some certs and reviewed controls. No known customer breaches, but probably replacement certs for the holders (minor).

2011. Website hack. A captive CA for a telecom had its website hacked, and subscriber information and private IP compromised (Goodin). Attacker was listed as a hacker who tipped off the media, claiming not to be the first. Parent telecom shut down the website.

2012. Weak Key scan. Two academic groups independently scanned the net for all published certificates (6-11 million examples) and analysed them (Heninger, et al) and (Lenstra, et al). They found that 1% of certificates were in common, and 0.4% were constructed with poor parameters which permitted the revealing of the secret keys. The keys were traced to 3 popular hardware devices that had one popular software package at its core. Consequences: Damages have not been assessed but would involve some rework and reputational loss by the suppliers of these devices. Gain in reputation for the academic groups.

2012. CA breached contract against MITMs. A CA announced that it had issued a subroot to a company for the purposes of intercepting the secure communications of its employees (SpiderLabs). This is contrary to contract with vendors and industry compact. At some moment of clarity, the CA decided to withdraw the subroot. Consequences: loss or damage to that customer due to contract withdrawal. Such contracts have been estimated to cost $50k. Destruction of the equipment concerned, maybe $10k. Loss of reputation to that CA, which specialises in providing services to US government agencies. Potential for delisting the CA concerned in vendors' trust lists which could be a bankruptcy event (TheRegister). Loss of time at vendors which debated the appropriate response.

Annex 3 - Likelihood and Consequence Tables

A.3-1 Risk Rating Matrix

as calcuated by

*R = Likelihood * Consequences*

or more precisely:

$R = (L * C)^{0.5}$

Description of Likelihoods	Events per annum	Years per Event	Likelihood	Consequences								
				1	2	3	4	5	6	7	8	9
				No impact to business. Will likely not be measurable, under the noise level.		Impact will be discernible but will absorbed in business costs.		Consequences will lead to costs, but are bearable.		Will cause significant costs which will have widespread impacts on different areas.		Bankruptcy Event. You are out of business.
Monthly event: this is certain part of the normal business process, and is a cost of business. There is no risk, it is a certainty.	10	0.1	**9**	3	4	5	6	7	7	8	8	9
	3.1	0.3	**8**	3	4	5	6	6	7	7	8	8
1 year event: plans must be in place to deal with this, and direct mitigations to offset the risk should be employed.	0.9	1	**7**	3	4	5	5	6	6	7	7	8
	0.3	3.1	**6**	2	3	4	5	5	6	6	7	7
10 year event: This will happen in the lifetime of the organisation's product & personnel mix, and would need to be addressed in planning, and probably mitigated at least to a limited extent.	0.09	10	**5**	2	3	4	4	5	5	6	6	7
	0.03	32	**4**	2	3	3	4	4	5	5	6	6
100 year event: it is possible, and probable to someone in the industry. It may be important to mitigate, or acceptable to ignore, depending on the wider context.	0.009	100	**3**	2	2	3	3	4	4	5	5	5
	0.003	316	**2**	1	2	2	3	3	3	4	4	4
1000 year event: this risk can be safely accepted.	0.0009	1000	**1**	1	1	2	2	2	2	3	3	3

Loosely modelled on srmbok pp137 Fig36.

A.3-2 Threat Matrix		Intent								
		1	2	3	4	5	6	7	8	9
		Off the agenda. Any discussions will be rhetorical, posturing, speculative.		Some contingencies are build, for opportunities. No timelines, few resources allocated.		Planning and preparation is in progress but competition exists and timelines are uncertain.		Substantial planning progresses to firm timelines, but may be distracted by other more important things.		All resources devoted, planning committed, all other priorities ignored.
Capability		1	2	3	4	5	6	7	8	9
9	*All tools at hand, and knowledge to use them. Almost trivial.*	3	5	6	7	7	8	8	9	9
8		3	4	5	6	6	7	7	8	9
7	*Good range of tools, and no difficulties with employment - can source any shortfalls without much difficulty.*	2	4	4	5	5	6	7	7	8
6		2	3	3	4	5	5	6	7	8
5	*Reasonable set of tools, with some knowledge - and can solve most issues given time and patience.*	2	3	3	4	4	5	5	6	7
4		1	2	3	4	4	4	5	5	6
3	*Some ability to bring tools and knowledge to bear but will be slowed by large gaps.*	1	2	3	3	3	4	4	5	5
2		1	2	2	2	3	3	4	4	5
1	*No capability.*	1	1	1	1	2	2	2	3	3

A.3-3 Intent Matrix			Confidence								
			1	2	3	4	5	6	7	8	9
			Will not act unless handed on a silver platter, and even then may withdraw support.		Easily swayed, will chose easy path, including doing nothing.		Comfortable, but will chose most economic path. Difficulties will dissuade.		Strongly self-confident, not swayed by difficulties.		Supreme. Arrogant. Does not recognise difficulties.
Attention			1	2	3	4	5	6	7	8	9
9	*Obsession, to the level of ignoring other important factors.*	9	6	7	7	8	8	8	9	9	9
8		8	5	6	7	8	8	8	8	9	9
7	*Completely aligned, but capable of distraction for other important issues. Systematic, patient approach.*	7	4	6	7	8	8	8	8	8	9
6		6	4	5	6	7	7	8	8	8	9
5	*Highly focussed but also equally interested in other possibilities.*	5	3	4	5	5	5	6	6	7	8
4		4	3	3	4	4	4	5	5	5	6
3	*Moderate levels of attention but easily distracted to other priorities.*	3	2	2	3	3	3	4	4	5	5
2		2	2	2	2	3	3	3	4	4	5
1	*Does not rate a look.*	1	1	1	1	1	2	2	2	3	3

A.3-4 Capabilities Matrix		Knowledge								
		1	2	3	4	5	6	7	8	9
		Knowledge of words, not their meanings.		Some abilities that can be brought to bear, but cannot bring cohesive set of abilities together.		Credible experience and theory brought to bear from other areas, some shortfalls and blindspots.		Strong experience in related fields, does not make mistakes.		Mastery, decades of direct experience, knowledge internalised.
Resource		1	2	3	4	5	6	7	8	9
9	*All the benefit of an industrialised economy made available for multiple, asymmetric, synchronous events.*	4	6	7	8	8	8	9	9	9
8		3	4	5	6	7	7	8	9	9
7	*Organisational machine with strong experience in supporting similar tasks.*	2	3	4	5	6	7	7	8	8
6		2	3	4	4	5	5	6	7	8
5	*Wide range of support that can be turned to the task at hand.*	2	3	3	4	4	5	5	6	7
4		1	2	3	3	4	4	5	5	6
3	*Some elements that support the task, but gaps are evident.*	1	1	2	3	3	3	4	4	5
2		1	1	1	2	2	2	3	3	4
1	*The task is easily overwhelmed, words and posturing more than actions.*	0	1	1	1	2	2	2	3	3

A.3-5 Attention Matrix Attention is an input into Threats, deriving from an Agent's attraction to a Scenario, and his inherent Desire			Attractiveness								
			1	2	3	4	5	6	7	8	9
			unimportant.		helpful but not strong.		scenarios can assist strongly.		attack scenario meets major goals.		scenarios are perfect.
Desire			1	2	3	4	5	6	7	8	9
9	*life goal, yin & yang.*	9	6	7	7	8	8	9	9	9	9
8		8	5	6	7	7	7	8	8	9	9
7	*organisation mission with serious thought.*	7	5	5	6	6	7	7	7	8	9
6		6	4	5	6	6	6	6	6	7	8
5	*important enabling step to wider objectives.*	5	4	4	5	5	5	5	5	6	7
4		4	3	3	4	4	4	4	5	5	6
3	*somewhat interesting or related to objectives.*	3	2	3	3	3	3	4	4	5	5
2		2	1	2	2	2	3	3	3	4	4
1	*unimportant, may be even damaging.*	1	0	1	1	1	2	2	2	3	3

Annex 4 - Risk Register, Treatment Schedule and Plan

RISK REGISTER										RISK TREATMENT SCHEDULE & PLAN											
Risk	Risk without Any Treatments (Inherent Risk Level)			What are Existing Controls? (Project 1)	Risk with Existing Treatments (Residual Risk Level)			Treat Risk?	Risk Pri	Revised Treatment Options (Project 5)	Risk with New Treatments (New Residual Risk)			Cost - Accept?	Implementation (Deferred pending Board Decision)		
	Con	Lik	Ris		Con	Lik	Ris				Con	Lik	Ris		Resp	When	Who
S.2 walk *disappearance of key person or partner.*	7	4	5	M.1: dual control M.18: Arb M.19: Redundancy	6	3	4	no	2	M.5: offline M.16: dup-ss	6	2	3		x	x	x
S.3 defect *change of loyalty of key person or partner.*	7	4	5	M.1: dual control M.2: FDE M.7: hisec-host M.8: soft M.17: ceremony M.18: Arb M.19: Redundancy	6	1	2	no	3	M.4: HSM M.5: offline M.16: dup-ss	6	1	2		x	x	x
S.5 legal *legal attack on key person, partner or self.*	7	3	5	M.1: dual control M.2: FDE M.7: hisec-host M.8: soft M.9: audit M.18: Arb	6	2	3	no	3	M.4: HSM M.16: dup-ss	6	2	3		x	x	x
S.6 hard *prepared hardware snuck into system*	7	6	6	M.1: dual control M.7: hisec-host M.9: audit M.17: ceremony M.18: Arb	6	3	4	no	2	M.4: HSM M.5: offline	6	3	4		x	x	x
S.7 soft *change or hack of software snuck into system*	8	6	7	M.1: dual control M.7: hisec-host M.8: soft M.9: audit M.17: ceremony M.18: Arb M.19: Redundancy	7	3	5	no	4	M.4: HSM M.5: offline	7	3	5		x	x	x
S.8 rep *deliberate reputational attack, including false breach claim*	7	3	5	M.7: hisec-host M.8: soft M.9: audit	6	2	3	no	5	M.4: HSM	6	1	2		x	x	x
S.9 FUD *Published noise on vague security basis such as Numerology*	7	3	5	M.9: audit	6	2	3	no	5	M.4: HSM	6	2	3		x	x	x
S.11 BreachD *Breach and theft of personal data or certs via website*	8	5	6	M.2: FDE M.7: hisec-host M.8: soft M.9: audit	7	3	5	no	2	M.4: HSM	7	2	4		x	x	x
S.12 BreachK *Breach and theft of root or subroot (software)*	8	5	6	M.1: dual control M.2: FDE M.7: hisec-host M.8: soft M.9: audit M.17: ceremony M.19: Redundancy	6	2	3	**YES**	**1**	M.4: HSM M.5: offline	6	2	3	M.4 30000 YES M.5 13000 YES sum **$43000**	x	x	x
S.13 Crypto *Weakness exploited in Cryptography or Algorithm to reveal key data: PKI, TLS, x509, RSA, SHA1, SHA2, MD5*	7	3	5	M.2: FDE M.8: soft	7	2	4	no	2	M.4: HSM M.5: offline	6	1	2		x	x	x
S.17 recovery *permanent unavailability of root by recovery methods*	7	5	6	M.1: dual control M.7: hisec-host M.8: soft M.9: audit M.17: ceremony M.18: Arb M.19: Redundancy	6	3	4	**YES**	**1**	M.4: HSM M.16: dup-ss	6	3	4	M.4 30000 YES M.16 12000 YES sum **$42000**	x	x	x

Following risks dropped for lack of priority: S.1, S.4, S.10, S.14, S.15, S.16

Annex 5 - Terms & References

Terms

Term	Definition	Reference
CA	A *Certification Authority* issuer of digital certificates that contain a statement of name of a holder, signed by the Authority.	
Certificate	A digital packet of information that typically includes the name of a person, a public key, and other technical data to help establish secure communications. It is (typically) signed by a CA.	
RA	A *Registration Authority* verifies the information to be placed in a certificate (name).	
Resources	Capacity, tools, assets or commodities available to a threat actor for achieving a particular goal. May be intangible (weapons, tech, people) or intangible (sources of funds, power, influence).	srmbok1#364 paraphrased
WoT or *Web of Trust*	A high-level term to describe a network of people, interlinked by assessments or claims (typically, Identity) over each other.	

References

Ref	Citation
Sotirov	Sotirov et al, "MD5 considered harmful today -- Creating a rogue CA certificate," http://www.win.tue.nl/hashclash/rogue-ca/
Black	Daniel Black, "Risk Assessment for CAcert," 2009, http://wiki.cacert.org/RiskAssessment
CAcert stats	CAcert Inc, "Statistics," online realtime report http://www.cacert.org/stats.php
DRC	David Ross, "Certificate Authority Review Checklist," 2005-2007, http://rossde.com/CA_review/
DSD	Defence Signals Division, Australian Government, http://dsd.gov.au/
History	CAcert, "History of Threats," wiki page 2012,
FC 1343	Ian Grigg, "Measuring Cyberfraud, the fall rate of sky, and other metrics from the market for Silver Bullets," 13 Nov 2011, Financial Cryptography blog post http://financialcryptography.com/mt/archives/001343.html
Fox-IT1	Fox-IT, 'DigiNotar Certificate Authority breach "Operation Black Tulip" ' 05 Sep 2011, Fox-IT, Audit of DigiNotar, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf
Fox-IT2	Michael Sandee, "RSA-512 Certificates abused in the wild," Fox-IT 2011 http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/
Goodin	Dan Goodin, "Digital certificate authority suspends ops following breach - Hackers access database, gain control over website," 8 Dec 2011, The Register, http://www.theregister.co.uk/2011/12/08/certificate_authority_hacked/
Grigg1	Ian Grigg, "The Maginot Web," 20 Apr 2003 Cryptography forum post, http://iang.org/ssl/maginot_web.html
Guerin	Gregory Guerin, "Microsoft, VeriSign, and Certificate Revocation", 20th Mar 2001, http://amug.org/~glguerin/opinion/revocation.html
Gühring	Philipp Gühring , "CAcert Threat Model," CAcert internal paper, http://svn.cacert.org/CAcert/SecurityManual/RiskAnalysis.pdf
KJE	Keith Joyce, "CPP50607 Diploma of Security and Risk Management - Working Manual" V1 Jul 2010, ASEC Pty Ltd.
Leyden	John Leyden, "CA issues no-questions asked Mozilla cert," 28 Dec 2008, The Register
NRTF	CAcert's New Roots Task Force, documentation and project, http://wiki.cacert.org/NewRoots
NRTF-P3	http://wiki.cacert.org/Roots/EscrowAndRecovery/SSSS http://wiki.cacert.org/Roots/EscrowAndRecovery/MultiMemberEscrow http://wiki.cacert.org/Roots/EscrowAndRecovery/ActorPassword
NRTF-P4	Project 4 is taken from these proposals within NRTF http://wiki.cacert.org/Roots/EscrowAndRecovery/Notary http://wiki.cacert.org/Roots/EscrowAndRecovery/EnvelopeBankNotaryEscrow
NRTF-P5	Project 5 is from this NRTF proposal http://wiki.cacert.org/Roots/EscrowAndRecovery/RedundantServers
Tänzer	Michael Tänzer, *The Influence of the Architectural Style on Security, Using the Example of a Certification Authority*, 2012 (unpublished diploma report, work in progress)
SP	Ian Grigg (Editor), "Security Policy," 10th May 2010, CAcert Policy http://svn.cacert.org/CAcert/Policies/SecurityPolicy.html
srmbok	Talbot & Jakeman, "Security & Risk Management - Body of Knowledge," 1st Edition 2008, Risk Management Institute of Australasia Limited.
wikipedia1	Wikpedia.com, articles on Verisign, GeoTrust and Thawte.
Zetter	Kim Zetter, "Hack Obtains 9 Bogus Certificates for Prominent Websites; Traced to Iran," 23 Mar 2001, Wired article http://www.wired.com/threatlevel/2011/03/comodo-compromise/

Figures

Annex 6 - Wider Observations on Methodology

Observations on Technical Calculations

The use of 3 factors - scenarios, agents and assets - and the existence of 10 entries or more in each of those registers resulted in a fairly large calculation set. As it was anticipated that this information be used in a real scenario, and updated from time to time, this indicated that an automated approach be useful.

However, in building the system and working with the data, some issues arose. Firstly, the amount of data continued to rise. Indeed, due to the combination effects from one factor to another, data rises at a rate far greater than linear. That is, adding one new asset requires data on that asset, but also values cross-referencing between the asset and all scenarios and all agents. Thus, data tended grows with the square of the size.

The number of existing mitigations was around 10, and tended to bring risks down quite significantly. As proposals were for only a few more mitigations - varying from 2 to 4 - these new mitigations did not achieve as much effect, suggesting an effect of diminishing returns.

Also, although the calculation was repeatable, it remained complex under the surface. This complexity generated its own artifacts. Typically, the projects tended to display a homogonisation of risk, with mitigations bringing all risk scenarios closer together in apparent risk level. This is either a reflection that the mitigations are working to balance risks, or that the calculations and risk tables are simply funnelling all the results together to the middle ground. In practice it appears to be a bit of both.

Finally, there are artifacts in the calculated analysis that suggest results at variance with expectations.

- The aggregated vulnerability for a scenario derives from the vulnerabilities of all assets to the scenario. In calculating the risk, this aggregated vulnerability leads to a higher risk where some lesser important asset (e.g., reputation) has a high vulnerability but lower consequences.
- Mitigations can effect the consequences and the effectiveness of various scenarios. But they can only marginally effect the likelihood (a locked house can move a thief to an unlocked house, until everyone has locks...). This results in a stubbonness of risks to not drop completely to ignorable. In the event, the total risk did not drop markedly and the conclusions had to rely on secondary effect, in this case availability.
- This leads to an alignment question across the calculations. Are levels comparative to each other? or are they comparative to the whole?

In conclusion, some observations can be drawn. It appears that a small scale risk analysis of say 2 factors and 5 entries in each of those registries can survive on paper. A medium scale risk analysis can do well with a moderate degree of data processing. However a large scale risk analysis, one that involves a substantial budget and group of assets, is likely going to be subject to swamping by complexity. Hence there would need to be some positive testing of its results. That is, some way to show that the analysis is producing viable conclusions is needed, not just providing an impenetrable faux-scientific veneer to guesswork, and consuming cranking costs into the bargain.

Opportunity versus Vulnerability

The difference between Opportunity, Targetability and Vulnerability is not entirely nailed down in the literature [srmbok]. In the analysis within, my definitions needed more clarity.

An Asset presents Opportunity. This can be measured in terms of Exposure times Accessibility, with Recognisability as an independent variable.

Then, Vulnerability is the exploitation by a Scenario of the Opportunity within an Asset to a greater or lesser degree. Thus, Vulnerability is found as a matrix of values between Assets and Scenarios, where each value is a modification of the Asset's Opportunity.

Effect of Mitigations

Mitigations related by threat scenario tended to combine to have quite strong effects on the Effectiveness of their chosen Scenario. A result often seen was that some measures such as Vulnerability, Opportunity, or Effectiveness were driven dramatically down, to the point where their import disappeared both from calculations and from effecting the risk. Which is to say, these intermediates were often reduced to a point where new mitigations had little apparent effect.

Whether this was as a result of truly mitigating the risk, or as a result of the approximations of risk calculations overshadowing subtle improvements was a call that was difficult to make objectively.

The Goal of Recovery and Indirect Consequences

The goal of this risk assessment was to advise on methods to improve the recovery prospects - a persistent, high priority need for the CA derived from audit prioritiies. This goal ran against two effects.

Firstly, most mitigations that sought to improve recovery outcomes also increased the risks to direct assets of the system. Especially, the root and data were subject to increased risks, literally as more copies were escrowed for recovery purposes. Hence the project became one of minimising the increase to risk, rather than decrease the risk.

Secondly, recovery (or more properly, failure to recover) itself was not an attack or hazard, nor was it a direct consequence of any given attack. Failure to recover is however an indirect consequence. Recovery is in a sense a mitigation for a broad range of attacks, yet the link between recovery-as-mitigation to any particular attacks is indistinct, and modelling is difficult.

In the event, the tools used were not capable of modelling indirect linkages; the tools correctly identified that recovery failure was an indirect consequence and therefore downgraded the effectiveness of this attack. For these reasons, the consequences of recovery itself -- the very goal of the assessment -- struggled greatly to make itself felt in the models.

Financial Modelling - open source, CAPM's discount factor, and benefits

All of the costings for projects and mitigations were estimated. There were several difficulties in this. Firstly, the majority of resource applied by an open source organisation is volunteer labour, something that is hard to cost. Direct monetary costs while important do not capture the real costs to the organisation, and nor do simple techniques such as allocating a money amount or "consultant's billing price" to time spent.

Secondly, in similar mode, many of the mitigations had serious on-going costs. For this purpose those costs needed to be discounted back to the current time in order to make any comparison valid. This then necessitated calculation of CAPM's discount factor. Calculations suggested the market discount factor be 5.5% (based on 0.25 risk free rate, betas from 4 similar companies averaging to 0.88 and a market premium of 6%) or 11% for an Open Source premium. Using my own judgement, 20% was used instead.

Thirdly, while the costs of mitigations were estimated, this is literally only half the story of a *cost-benefit analysis*. To complete the picture, costs need to be subtracted from benefits of each mitigation to give a netted result. This was added to the modelling, but the numbers were found to be very sensitive to the inputs, undermining the robustness of the recommendations. More work would be required to expand the mitigations with more data and modelling to get better outcomes from cost-benefit analysis, and the results are not presented here.