Password recovery policy	Chris P., Guillaume R.
WIP	$Date: 2007-10-07 22:00:00 +0200 $

1 Scope and Purpose

As subscribers loose their passwords, often because of their own mistake, CAcert provides the subscribers with several ways to recover their password.

CAcert Support needs to ensure the confidentiality and safety of the procedure.

Nevertheless, CAcert acting as much as possible as a robot CA has to minimize the workload of its support team members. So CAcert offers automatic & manual procedures.

2 Password recovery procedures

2.1 Automatic password recovery

2.1.1 Client certificate login

The prefered way to recover a password is to use a CAcert signed client certificate to login to CAcert. No password will be needed and the subscriber has full access to his account.

After suscriber login with a client certificate, the subscriber can reset his 5 Lost Password Questions to change his password using 2.1.2.

2.1.2 Lost Password Questions and Answers

Every subscriber is required to setup 5 lost password questions and answers on registration and will be reminded to do so on every login, if there are less then 5 questions saved in the database.

To recover a password, the subscriber has to correctly answer three questions, randomly chosen out of all five. *The subscriber has “unlimited” tries (exceptions see Abuse Cases)*.

The check is performed case insensitive and leading or trialing spaces are removed.

If all three answers are correct, the password will be updated.

Otherwise the system administrator will be notified.

See Lost Password Questions answered with minor errors

See Lost Password Questions answered wrongly

2.1.3 Account recovery by dispute

A subscriber can choose to give up his old account and create new one using a different email address. All domains and email addresses verified for the old account can be put

into automated dispute system to release them from the old account.

All certificates set up within the old account will be revoked. All assurance points are lost.

2.2 Semiautomatic password recovery

2.2.1 Password recovery logging

CAcert logs all tries of automated password recovery. Support team has to watch frequently thoses logs in order to figure out if attackers tries to hijack subscriber accounts.

2.2.2 Lost Password Questions answered with minor errors

If a subscriber fails to answer all questions correctly, the support team will be notified by email, quoting the answers stored in the database compared to the answers given by the subscriber for password recovery.

If both answers have only minor differences (single missing character, one is a short form of the other) and there is no doubt that the meaning of the answers is the same, the system administators should assist the subscriber as described in § 3.

It the subscriber uses the lost password form multiple times and in total there are three correct answers multiple emails, the system administrators should assist the subscriber. This doesn't apply if the answers give the impression that the subscribers was guessing several different words.

2.3 Manual password recovery

2.3.1 Lost Password Questions answered with minor errors

[proposal : removal of this paragraph because this task is time consuming. (Guillaume Romagny USO October 7th 2007)]

If the System Administrator notices multiple password recovery tries using the Lost Password Questions function, he should ask the subscriber if he needs assistance.

The password should never be updated automatically as

- the subscriber might have found the correct answers and updated the password already

- the subscriber might have remembered his old account password

If system administrators update the password anyway it might introduce further problems.

A possible offer of assistance may be "I saw that you tried to updated your CAcert password and noticed that your're using a short form of your girlfriend name instead of the full name. You might want to try again." "Your answers to the Lost Password Questions were almost correct - do you want me to update your password manually to the new password you tried to set or did you find another solution yourself?"

2.3.2 Password update request

If a subscriber fails to recover his password, he may apply for support by donation.

This means, that he has to donate money or work worth about $US 15 to CAcert, the CAcert wiki, support mailinglist, Translation, etc.

He needs to provide proof of this donation when requesting the password change.

Suscribers willing to request a manual password recovery must send a request to support (at) cacert.org

If a subscriber requests support to set a new password, he has to provide the following:

- a proof of donation (as described in § 2.3.1)
- a proof of identification (image of passport or ID card)

The administrator should act upon this request as soon as possible and email a new password to the account owner.

- A password provided by the subscriber must not be used.
- The password has to be emailed to a verified email address for that account.

As long as the subscriber fails to provide the required items, the change may not be processed.

If a subscriber has no trust point, the checking of the photo id is not required.

If the subscriber is also an organisation admin, Support team has to email the others admins of the organisation (if any) to keep in touch with the subscriber to check if everything is ok.

3 Renewing subscriber password

1.1 Quality of passwords provided

Support has to ensure the unicity, the quality of the randomness of the password provided and make sure the email containing the new subscriber password is ciphered.

The Security Officier (or Support Officer as a back-up or if the task is delegated) must validate the methods to generate new passwords and send ciphered emails to the subscribers.

1.2 Preserving password security after recovery procedure

When providing a new password, support team should avoid using the keyword “password “ (or any related keywords) in the reply mail if the email cannot be ciphered for any reason.

In all cases, the Support team has to request the subscriber after he/she has recovered his CAcert account with the new password to change this password as soon as possible, to check/provide the 5 questions & answers, to generate and keep safely a new client certificate to login to his/her account.

4 Abuse Cases

4.1 Multiple recovery tries using Lost Password Questions

Depending on the number of tries to recover the password :

- If the logs contains more than 15 failed tries to recover a lost password, the support team has to inform the account owner with no delay,
- The account may be blocked by changing the Lost Password Questions to random values if there are more than 50 failed tries.

4.2 Technical Problems

In the case that due to database problems an account has been set in a state where login and/or password recovery is impossible, CAcert should give the subscriber every possible support to access his account again and as soon as possible.