



Password challenges: Security and costs!

Finn Jensen, CEO FastPassCorp Dec. 2010.

Passwords are by far the most frequently used method for user authentication. Password authentication is fast and cheap, and password authentication is standard for practically all IT systems and applications.

It is therefore of vital importance that passwords and processes around passwords are secure. IT security officers see a number of threats to IT security through the misuse of passwords. Mitigation against these threats can often lead to cumbersome and expensive processes, in contrast with the original idea of passwords as a fast and cheap authentication method. Modern self-service tools such as FastPass, on the other hand, offer technology which improves security and reduces the total cost of the password processes!

It is generally agreed that IT security policies must control who is allowed to access specific information. To enforce such a policy it is of vital importance that the IT system and processes are secure, and that users are correctly identified and authorized. Passwords are still the primary key for authentication! It is therefore crucial that passwords effectively secure the authentication of the correct person. Of course this also has to be done at the lowest possible total cost!

This document describes the challenges and solutions for the use of a password, from a security and economic point of view.

What is the original reason for the use of passwords? It was, and still is, to tie a 'real' person to a user-id, which is the only identification an IT-system can use. As a password is supposed to be personal and secret, then only the 'real' person can activate their own user-id. With this user-id we can then make a person responsible for the actions of their user-id.

This, however, requires that the password is personal and secret. To achieve this and prevent misuse of passwords more and more demands have been put on the construction of passwords and the processes around passwords. What is visible to the user is longer and more complex passwords and frequent changing of passwords, which also have to be different from previous passwords! Of a more technical nature is the requirement for encryption during transmission and storage. The processes concerning the rendering and resetting of forgotten passwords also have to be very rigid when it comes to authentication of the receiver of the new password and the transportation of the password to the user.

The more security we want to build into the process the more expensive it usually gets.

These challenges of security and costs should lead to a review of the challenges and possible mitigation available for modern IT departments.

Inspiration can be found in the document: Special Publication 800-118 (Draft); **Guide to Enterprise Password Management** (Draft); Recommendations of the National Institute of Standards and Technology.

Weak links of Passwords

In well run IT operations you will see users be required to have a very complex password with frequent changes. Many users will even have many different passwords to remember, which complicates life even more. As a result of this, some users help themselves by noting passwords on yellow stickers to be sure they can sign-on without delay!

An overview of the challenges with passwords and potential result of weak links are listed in the table below. We have also listed some possible mitigation tactics, and their potential consequences.

Mitigation and consequence in traditional and manual systems

Weak links	Result	Mitigation	Consequence of mitigation
Password guessing	Security breach	Long and complex passwords. Lock the account after a limited number of retries.	Users forget or write on yellow stickers.
Password sniffing / cracking	Security breach	Encryption & secure communication.	Cost.
2nd person involved in password issuance and password reset	Security breach, Productivity loss	Strict control of people and processes. Self-service password reset.	Outsourcing might not be a good idea!
Forgotten passwords	Productivity loss	Simple passwords with no change and history!	'Broken' password confidentiality.
Yellow stickers!	Security breach	Simple passwords with no change and history!	'Broken' password confidentiality.
A stolen password can be reused without the user knowing	Security breach	Inform of last login. Notification of logins.	Cost to change application.

As seen in the above table the mitigation tactics often lead to new challenges and the problems just kind of rotate!

What is needed is a complete change to some of the basic processes around passwords.

The basic problem is that complex passwords mean that users forget passwords. Then the users either write on yellow stickers or call the HelpDesk, which is embarrassing and costly.

FastPass for User Self-service.

What is needed is to make life easy for the user if the password is forgotten. In that case IT security can have complex password policies, and users will not need yellow stickers!

The technology which makes it easy for the users is User Self-service of Password Reset. If a user can reset a forgotten password in less than a minute without calling the HelpDesk then it is acceptable for the user, and it carries no cost for the company!

If we look upon the challenges listed in the above table, but introduces FastPass for Password Self-service then the results come out quite differently!

Mitigation and consequence with FastPass Password Self-service

Weak links	Result	Mitigation	Consequence of mitigation
Password guessing	Security breach	Long and complex passwords. Lock the account after a limited number of retries.	Users change password in FastPass when forgotten.
Password sniffing / cracking	Security breach	Encryption & secure communication. Limit number of retries.	Cost
2nd person involved in password issuance and password reset	None: No second person is involved with FastPass		
Forgotten passwords	None: Users change password in FastPass when forgotten		
Yellow stickers!	None: No need for yellow stickers when FastPass is easy to use		
A stolen password can be reused without the user knowing	Security breach	Inform of last login. Notification of logins.	Cost to change Application

Out of the six weaknesses FastPass has solved three. The mitigation for Password guessing will also now be effective. With FastPass Self-service Portal for Passwords the majority of issues and problems with passwords are solved!

For most companies the cost of resetting passwords in a HelpDesk is 2–3 times that of the cost of resetting passwords with FastPass, so with the aim of increasing password security costs are even reduced at the same time!

Making the password reset process secure!

When a user resets a forgotten password in FastPass, IT security policies will define how the user authenticates himself.

For a security-sensitive system like FastPass you will, in most cases, require strong authentication by the user before they are allowed to reset their passwords. Strong authentication is achieved when two different methods are used in the same process. FastPass has the following four methods:

Something you know: Private and personal questions (1–9 questions).

Something you have: Your mobile phone as token (A PIN-code is sent via SMS to authenticate for FastPass).

A place you are: Secure IP-addresses.

Something you are: A personal interaction with a HelpDesk employee.

The FastPass administrator can define different authentication processes for different users, and even for the same user in different situations. As an example a user on a secure IP-address might only have to answer some challenge questions, where the same user from an unsecure network will have to use the SMS PIN-code AND challenge questions to be authenticated.

The technical security is protected via encryption and hashing of challenge questions, and secure communication protocols for all information flow.

In addition any transaction in FastPass can be notified to the user. This enables early warning to the user if another person is trying to get access to his password resetting services.

The conclusion: With FastPass Password Self-service IT departments can increase IT security and reduce costs simultaneously.

