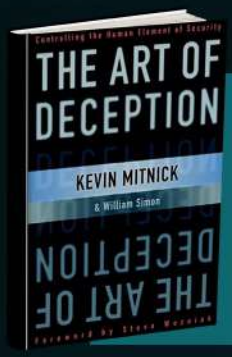
FASTPASSCORP

Identity Verification Manager

IVM secures the password reset process of Service Desks

⚠ ISSUE:

When users forget their password, they can only reach the service desk by phone – because, of course, they can't get it from their PC! The service desk agent must then ***verify the identity of an unknown user from only their voice.***



> "Why should an attacker ***spend hours trying to break in***, when he can do it with a simple ***phone call*** instead?"

If we want to take human error out of the identity verification equation, we must have an IT workflow controlling the agent. The process must be designed according to security specifications from IT security. There should be different processes for user groups with different security profiles. The tests must include many different items: data, tokens, and even manager approval, where needed

CONCLUSION:

The ***password reset process at the service desk*** can be an excellent gateway for hackers to breach IT systems.

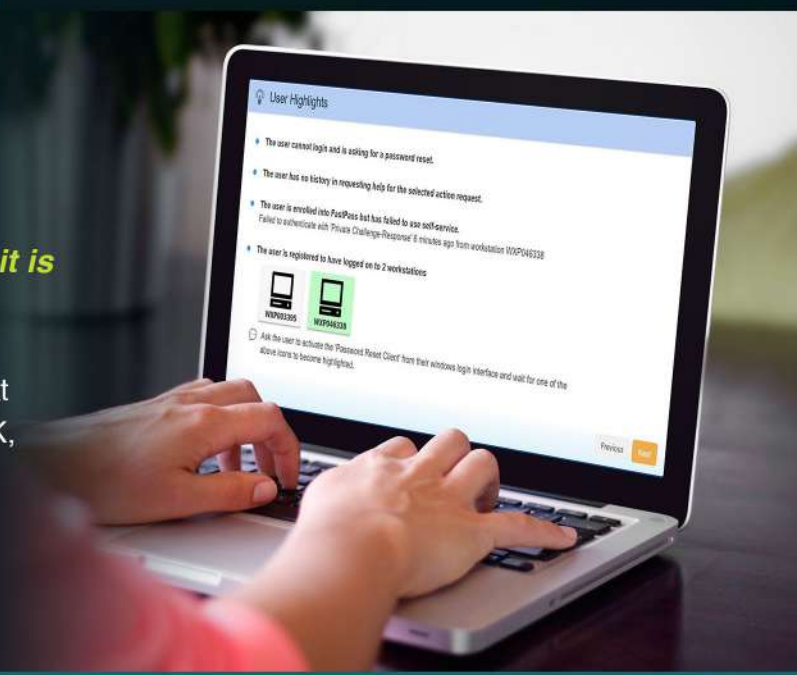
About IVM

Identity Verification Manager

The critical part of the password reset process is **identity verification.**

How can the service desk agent confirm that it is the legitimate user?

This task is taken over by IVM, which will control what actions to take and decide when the verification is OK, based on specific knowledge about each user.



Management-approved process

The process is decided upon by management – in most organizations, by the IT security department. The decision is no longer based on the service desk agent's judgment. IVM can be configured individually to the organization's security requirements.

Different verification processes for different groups

To gain acceptance among user management, the verification process should be as streamlined as possible. Some users with access only to low sensitivity information can be handled with a short and simple process. Executives and other key employees will be asked to give more information, to increase security.

IVM can provide an unlimited number of different processes linked to user groups.

Many verification options

IVM can use many different tests to verify the identity of the person:

Secret personal information

If the user has entered personal, individual information, then we can ask questions related to this. IVC even prevents the service desk staff from looking up the answers! The information can be gathered as part of the enrollment process for FastPass Self-Service clients.

Company information

Information from the Active Directory and from other internal systems can be used, too. The weakness of this resource is, of course, that this data might be available to others with the right access.

Tokens

IVM can communicate with many different user tokens, including mobile phone/SMS, private e-mail, authenticators from Microsoft, Google, and DUO, RSA tokens, SMART cards, and more. Note, however, that if self-service for passwords is implemented, then the user probably could have used self-service!

Contextual and dynamic information

To prevent hackers from preparing answers for key employees, IVM adds contextual and dynamic data that changes continuously and is very specific to the individual.

Examples are:

- Is it your PC?
- This is an unusual geo-location.
- When did you log off yesterday?
- Is this your normal meeting time?

Manager approval

IVM can include one of the strongest verification tests: The user's manager's verification that the employee is truly waiting for a password. This can then be confirmed in an integrated IVC process.

Delivering passwords to the user

When IVM has given the user enough points for verification, ***it provides the service desk agent with an interim password for the user.*** This can be delivered over the phone or to the user via SMS or private e-mail.

Monitoring

Every step of the process is logged and available for monitoring and reporting.

Integration to ITSM tools

IVM can be integrated into most modern ITSM tools, so the service desk agent sees IVM as a natural, integrated part of the different services they provide to users.

IVM implementation

To achieve rapid results, IVM is delivered with templates that can be used as basic processes immediately. They correspond to a simple process, an average process, and a heavily secure process.

The templates can then gradually be altered or new ones can be added, as the service desk and IT security agrees that adjustments need to be made.

This means that IVM can be installed and implemented very quickly.

FastPass overview

Identity Verification Manager

The FastPass Identity Verification Manager suite currently covers:

- **FastPass Self-service Client (SSC)**
- **FastPass Identity Verification Manager (IVM)**

IVM relies on the data and components of SSC, so we recommend a combined solution. IVM increases security and reduces the risks of social engineering, while SSC delivers productivity and efficiency for both users and the service desk.

The combination of SSC and IVM is a security solution with a strong business case!

Do you want to see how you can create a secure **manual password reset process** for your service desk?

CONTACT US:

North America : + 818 697 2308
Europe : + 45 4810 0410
info@fastpasscorp.com
www.fastpasscorp.com