



DigitalPersona Product Brief

Sharing data securely with DigitalPersona® Pro

An introductory technical overview to the DigitalPersona solution for email and document signature and encryption.

December 2010

DigitalPersona Pro is a leading centrally-managed suite of security solutions that protects data and controls access to PCs and applications. It simplifies management of solutions like disk encryption, strong authentication, single sign-on, and more thus helping achieve compliance and lower security-related IT costs.

This document is intended to provide a high-level, technical overview of how DigitalPersona Pro's digital signature and encryption module works.

Protecting information in motion

A primer on Public Key Infrastructure

Protecting data that is shared among individuals can be challenging, because the system has to know which users are allowed to share an email or a file, and which users are not. Conceptually, this requires users who want to exchange a protected document or email to share some secret, like a common password, or to establish a special trust relationship between them that makes communication easy among trusted partners, but not accessible for other users.

Traditional encryption techniques that might be appropriate for data at rest – for example, data stored in the hard drive of a computer – however, may not work. Such techniques are sometimes referred to as *symmetric encryption*, because they require the same password or PIN to be used for both encryption and decryption. In the context of a shared email or file, they would require all users who need access to such data to share the password used for encryption. It is easy to imagine how impractical this would be in a real life scenario – the sender of an encrypted email would need to encrypt the message, and then tell the password to the recipients (e.g. with an unencrypted message, a phone call, or other methods) so that they can decrypt the message when they receive it.

This is why solutions such as DigitalPersona Pro's secure communication module use technology referred to as PKI (Public Key Infrastructure), which uses *asymmetric encryption* to overcome the challenges described above. PKI technology uses the concept of a pair of encryption keys, called *public key* and *private key*, which are associated to each user. As the names suggest, a user's public key is meant to be shared with the rest of the world, similarly to a person's phone number. On the other hand, the

private key should be kept secret and should not be disclosed to anyone.

Thanks to mathematical properties, users can use public keys to encrypt data, but only private keys can decrypt them. For example, if user A and user B want to share data securely, user A can use User B's public key to encrypt the data. User B, however, can only decrypt the data using his own private key, which is secret and not available to anybody else. If a malicious user – User C – stole the encrypted data, he would not be able to decrypt it without User B's private key.

Digital certificates and Public Key Infrastructure

Having clarified how Public Key Infrastructure can help solve the problem of encrypting data in motion among individuals, how can an organization associate a pair of public and private keys to each user? The most common method is to deploy *digital certificates* throughout the business. A digital certificate (sometimes referred to as *digital ID*), in fact, is an electronic document – a file – that associates a person with a pair of PKI keys. Digital certificates can be purchased from Certificate Authorities, who guarantee the validity of such certificates, or they can be self-generated within the organization using tools from vendors such as Microsoft®.

If you do not know how to go about purchasing and deploying certificates, make sure you ask your DigitalPersona representative. They will be glad to help you find the solution that best fits your needs.

For purposes of this product brief, we will assume your company's IT Department deployed digital certificates to all of your users.

Once such certificates are deployed, two more things need to happen in order to protect information in motion within your organization:

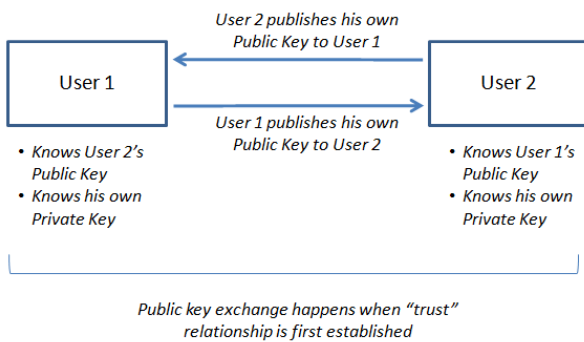
- First, IT or users need to establish trust relationships between users that need to share information securely, based on digital certificates
- Then, IT needs to be able to define how employees authenticate when signing or encrypting email and documents

At this point, users can encrypt email and messages.

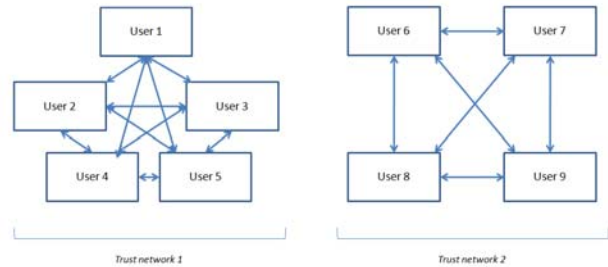
Establishing a trust relationship

DigitalPersona Pro’s secure communication module, Privacy Manager, allows not only IT but also users to build their circle of *trusted contacts* – i.e. other users whom they want to securely share information with. Users can build these trust networks by adding each others’ email address in the Privacy Manager trusted contact lists; or, IT can automatically make all users within the domain become trusted contacts.

When two users become trusted contacts, DigitalPersona Pro takes care of exchanging users’ public key information – similar to two users exchanging email addresses or phone numbers. These public keys will be used to encrypt email or documents, as described above.



At the end of this process, the organization will be either a single giant network of employees who all share each other’s public keys, or it will be fragmented into multiple mini-networks of employees that share information – often, based on their position in the organization, either by role in the hierarchy (e.g. Executives vs. middle-managers) or by department/function (e.g. Marketing vs. Manufacturing).



Defining user authentication

Once trust networks are created, IT needs to determine the mechanism that allows users to trigger the signature or encryption process. Such mechanism ties the user to his digital identity, therefore providing improved assurance the actual person signed or encrypted the document.

Rather than relying on passwords, which can be easily forgotten or compromised, DigitalPersona Pro allows IT to configure strong authentication policies that users have to fulfill when signing and/or encrypting an email or a document.

IT Managers can choose from a broad range of policies, ranging from no authentication (i.e. Single Sign-On) to multi-credential authentication with methods such as biometrics or smart cards. Each option provides unique characteristics and user experiences and should correspond to the balance between security and convenience IT Managers deem appropriate for the organization.



Encrypting email messages and documents

Once digital certificates are in place, trust networks are created and authentication policies are defined, users that need to exchange secure messages within their trust network can sign and/or encrypt the email or document using DigitalPersona Pro's Privacy Manager.

To perform the digital signature or encryption, Privacy Manager leverages digital signature and encryption functions built into supported productivity applications – such as Microsoft® Office® or Adobe® Acrobat® – to lock the email message or document. To trigger the digital signature or encryption, users can easily click on the Privacy Manager commands that seamlessly and automatically appear within Microsoft Outlook and Office upon installation. This ease of use greatly simplifies the user experience and lowers Help Desk calls.



The encrypted package of data – email, or document – is then sent to the intended recipient, together with the information needed to decrypt such package using his own Private Key. This helps protect information in case a message is lost or data is accessed by a malicious user, because he would not have access to the intended recipient's Private Key and therefore would be unable to decrypt the data.

More questions? Contact us

DigitalPersona is looking forward to hearing from you and answering your questions. Contact your Account Manager or sales@digitalpersona.com to learn more.

Disclaimer

THE INFORMATION IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO BE ANYTHING OTHER THAN THE EDUCATED OPINION OF THE AUTHOR. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT DIGITALPERSONA MAKES NO CLAIMS, PROMISES OR GUARANTEES ABOUT THE ACCURACY, COMPLETENESS, OR ADEQUACY OF THE INFORMATION. THIS INFORMATION SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. DIGITALPERSONA SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS OR COMPLIANCE WITH ANY LEGAL REQUIREMENTS.

© 2010 DigitalPersona, Inc. All rights reserved. DigitalPersona is a trademark of DigitalPersona, Inc. registered in the U.S. and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners. MC-113-121510