



ELECTRONIC SIGNATURE PRODUCT FAMILY

Signed Document eXpert



Electronic signature

Timestamping

Management of authentic documents

Electronic data and documents can be protected with authentication, ie the use of electronic signatures and timestamps.

The SDX product family is based on Public Key Infrastructure (PKI), a standard and widely used technology for electronic signatures.

Public Key Infrastructure:

- guarantees the identity of the signer (*authenticity*)
- makes impossible to deny the signature / document (*non-repudiation*)
- make impossible to alter the document unnoticed (*integrity*)
- protects against unauthorized access, encryption (*confidentiality*)

The SDX suite provides a comprehensive range of PKI based data protection tools used in electronic systems, from server applications to end users.

SDX products allow a comprehensive management of documents secured with digital signatures

- at the level of individual documents and files
- in messaging applications
- in browsers and browser based applications
- in document management and archiving systems
- in applications requiring one time or mass production or verification of electronic signatures.

SDX features:

- all components integrate smoothly with standard certificate authorities and timestamp authorities
- adapted easily to the individual requirements of a given organization or process
- localized to any specific legal and language requirements
- based on Electronic Signature Policy: the ESP defines how digital signatures are regulated in a given organization or environment, what standards and conditions exist for a document to become legally binding
- authenticity may also be checked using CRL or OCSP services.

Application Fields

Business case	Use
Electronic government	Secure document exchange A2A, A2B, A2C
Financial transactions	Encryption and authentication of financial transactions with digital signatures
Billing	Authentication and secure transmission of invoices and statements of accounts, B2B, B2C
Records management	Managing authentic documents
Order processing	Data protection of e business workflows and secure communication between parties
Health care, medical records	Protection of patient data, secure transmission
Legal documents	Authentication and secure transmission of documents
Corporate communication	Legally binding commercial and legal correspondence, B2B, B2C, B2A

SDX Components

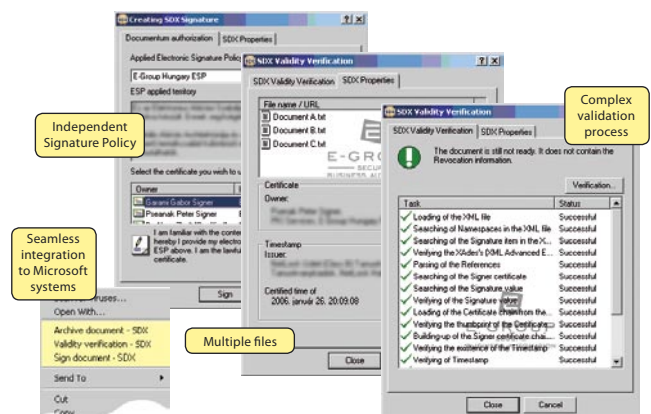
The SDX product family consists of several client and server side applications.

Client side components make easy the authentication and verification of documents:

- creation of electronic signatures, signing a document
- managing signature hierarchies
- managing timestamps
- verifying the authenticity of signed documents
- encryption

Client-side Components

Component	Short description	Function								
		Verification	Signature	Time-stamping	Encryption	Archiving				
SDX Professional	<ul style="list-style-type: none"> • general signature management functions • certified by an independent certification organization 	●	●	●						
SDX Browser	authentication of forms (XML) with a built-in plug-in	●	●	●						
SDX Archive	preparing authentic documents for long-term archiving (storing data proving authenticity)					●				
SDX Encrypt	encryption certificate is needed for encrypting				●					
SDX Enterprise	authentication and encryption in one process	●	●	●	●					
SDX Verify	<ul style="list-style-type: none"> • FREE signature verification tool • can be installed with an intelligent installer 	●								
Additional components										
SDX Scan Plug-in	<ul style="list-style-type: none"> • authentication of paper-based documents • available separately 									



Client side components are available in a package that:

- is Microsoft AuthenticCode and InstallShield compatible
- has a multilanguage user interface
- has an easy and robust setup process
- is Electronic Signature Policy – XADES compatible

Server Side Components

Main features:

- signing high volumes of documents
- compatible with Network Load Balance System (NLBS)
- black box strategy
- scalability
- cluster-ready
- open, standard interfaces
- robust application

SDX MultiSign Server

signing and time-stamping high transaction volumes
automatic, without human interaction
load-balanced
cluster-ready
NLBS-ready

SDX Mediator Server

speed up and cache electronic signature requests
signature proxy server
mediates closed corporate LAN to environmental and external CAs

SDX MultiSign Server Mediator Edition

multi-functional (proxy and signature server)
certificate revocation list caching
certificate based transaction queues
increased speed and reliability

SDX VerifyAll Server

verification of large transaction volumes
integrated time-stamping
embedded verification status

Licensing policy:

- transaction-based
- processor-based
- can be restricted to applications or organizations

SDX-based complex architectures

- applications with both client- and server-side components
- system interoperability
- clear and transparent system interfaces:
 - SOAP
 - HTTP
 - Message Queue: MS MQ, SUN and Java MQ
 - secure FTP
 - system monitoring interface (SMB, SysLog)

Mobile SDX

signing documents with mobile phone
wireless PKI and mobile GSM technologies in document authentication

SDX TransForm

full life-cycle of authentic form-based data exchange
based on SDX authentication and validation features
integrated document transaction life cycle
web-based document and form transmission

SDX add-ons for Exchange and for Notes

seamless integration with MS Outlook, Outlook Express and IBM Lotus Notes
toolbars
EU-conform signed mail
adaptation to local country regulations

Mobile SDX

Main features of the document authentication solution:

- mobile SDX extends SDX functionality to the wireless world
- signatures are generated by the mobile device using mobile and standard Internet-based transactions
- built on wireless PKI and mobile GSM technologies
- supports mobile devices, phones and PDAs
- state-of-the-art integration with wireless PKI SIM architectures and Microsoft operating systems
- mobile phone can be used as a personal trusted device
- SIM card-based X.509 certificate management
- certified Microsoft Cryptography Service Provider (MSCSP)



Application fields:

- supporting B2B, B2E, B2C, A2C and A2A communication processes
- creating authentic documents
- setting up secure SSL connections
- securing electronic identities for online services

To generate digital signatures, you usually need smart cards, card-readers, browser plug-ins, etc. So that digital signatures can be used widely.

Why to use a mobile phone and its SIM card to generate the digital signatures?

It has significant benefits:

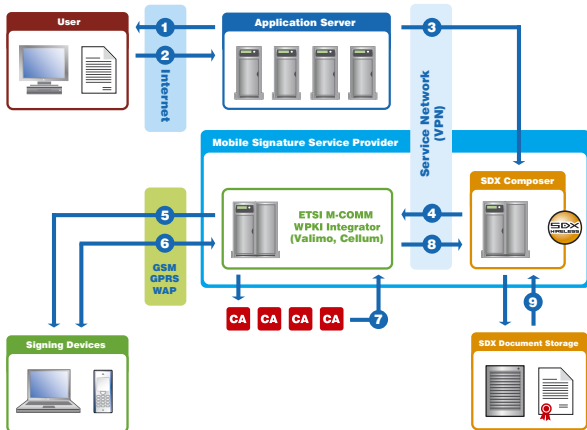
- the mobile phone is always with you
- there is a smart card (SIM) and a smart card reader in your pocket
- it is most personal
- you notice very soon if you lose it

Conclusion

A mobile phone is a convenient tool for strong user authentication and the creation of digital signatures. Such an integrated infrastructure can provide a Mobile Signature Service (MSS).

Joint product development

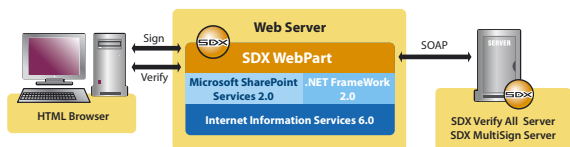
Mobile SDX is fully integrated with secure SIM and transaction delivery platforms (OTA extensions) such as **Valimo** (Cellum (Hungary) and Valimo (Finland) wireless architectures).



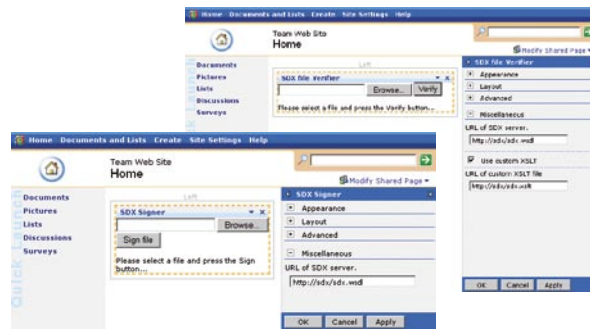
Workflow

1. presents the document to the user
2. prompts the user to sign a document (agreement, transaction etc.)
3. calls the signing service of SDX Composer
4. SDX Composer calls the wPKI Integrator signature creation service
5. wPKI Integrator sends the signing request with embedded data to the mobile device
6. the user creates the signature on his mobile phone and sends back the signature to the wPKI Integrator
7. wPKI Integrator checks the validity of the user certificate via CA services (CRL or OCSP)
8. wPKI Integrator sends back the signature and the validity data to SDX Composer
9. the SDX Composer completes the signed documents (generates the data in XAdES format and extends it with auxiliary data, optionally saves the document (timestamp, Signature Policy reference, other attributes)
10. the SDX Composer hands over the signed document to the application
11. the application notifies the user about the creation of the signed document

SDX Microsoft Sharepoint Server Integration



- SDX WebPart helps developers with integrating the Mobile Signature Service seamlessly with a Microsoft SharePoint Server
- WebPart enables MS Portal Server to manage both standard and mobile digital signatures and to integrate the signed documents with the portal presentation
- SDX VerifyAll and MultiSign server can be embedded into intranet and extranet portals



Selected SDX References

- Government Citizen Identification Portal
- Electronic Government Gateway – authenticating citizens
- Hungarian e-government administration: implementation of secure electronic customer communication, using SDX for authentication
- National Pension Fund – pension administration and declaration
- Hungarian Post Inc.– digital signature on large document store
- the Hungarian Ministry of Internal Affairs – National Archive of Local Regulation – authentic archive of regulatory documents
- MOL
- Drescher
- EBPP.HU

Supported Operating Systems

Microsoft® Windows®

Supported Standards

SDX product family standard compatibility list

IETF

- RFC 3161 Internet X.509 PKI TSP
- RFC 3279 Algorithms and Identifiers for the Internet X.509 PKI Certificate and CRL Profile
- RFC 3280 Internet X.509 PKI: Certificate and CRL Profile
- RFC 3739 Internet X.509 PKI: Qualified Certificates Profile
- RFC 2560 Internet X.509 PKI: OCSP

ETSI

- SR 002 176 Algorithms and Parameters for Secure Electronic Signatures
- TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
- TR 102 038 XML format for signature policies
- TS 102 023 v.1.2.1 Policy requirements for time-stamping authorities
- TS 101 903 v.1.2.2 XML Advanced Electronic Signatures (XAdES) (XAdES-EPES, XAdES-TS, XAdES-C, XAdES-A)
- TS 101 862 v.1.3.1 Qualified Certificate Profile
- TS 101 861 v.1.2.1 Time Stamping Profile

CEN

- CWA 14170 Security requirements for signature creation applications
- CWA 14171 General guidelines for electronic signature verification
- CWA 14365 Guide on the Use of Electronic Signatures - Part 1 and Part 2

If you have more questions about the SDX Product family, our colleagues are happy to provide you with more information.



E Group

Address: Hauszmann u 3/a, Budapest 1117, Hungary, Europe
Phone: (+36-1) 371-2555

E Group ICT Asia Ltd.

Address: The Gateway, 25 Canton Road, Tsimshatsui, Kowloon, Hong Kong
Phone: (+852) 986-08871

