Ing. Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security | CEHv7 |
ondrej@sevecek.com | www.sevecek.com |

CRYPTOGRAPHY

1

Outline

- Hash algorithms
- Symmetric algorithms
- Asymmetric algorithms
- Timestamping
- Random number generators
- Current algorithms in use
- Cryptographic standards
- SSL/TLS
- Operating system support

2

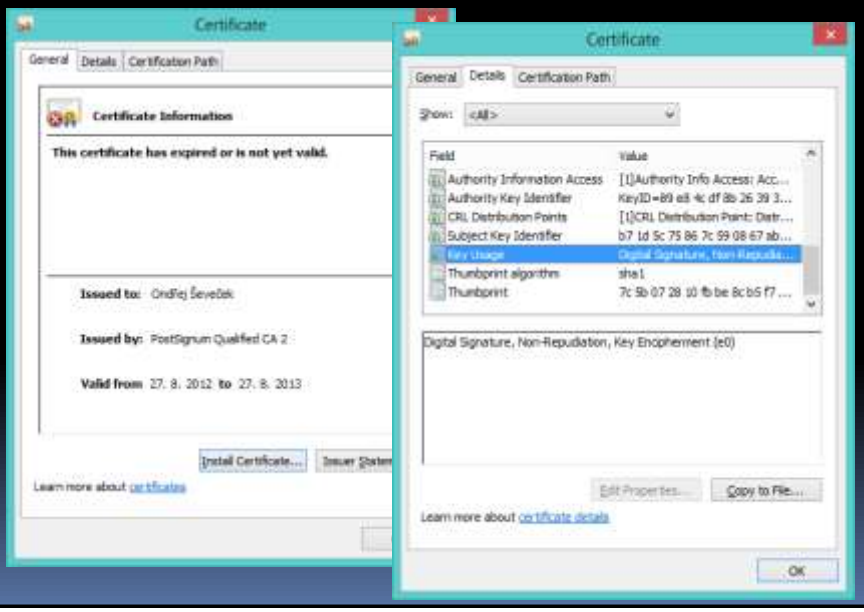
What is information security

- ISO 27002:2013
- the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)

Security services

- Confidentiality
- Data Integrity
  - accidental vs. deliberate modification
- Authentication
  - plus role-based authentication when more individuals share authentication information
- Authorization
- Non-repudiation
  - responsibility to keep signing keys in private
- Time stamping

Example: Non-repudiation



Example: Authentication without Confidentiality

- Authenticated HTTP
  - SharePoint or CRM by default
- Share files (SMB)
  - cannot be encrypted at all (would have to use IPSec)
  - can be signed with Kerberos/NTLM session keys
- LDAP
  - most LDAP AD queries require authentication
  - most Windows applications do not encrypt LDAP
  - can be encrypted/signed with Kerberos/NTLM session keys

Example: Confidentiality without authentication

- RDP Security Layer
- Diffie-Hellman (DH) key exchange
- Safe against passive eavesdropping
- Active MITM can decrypt everything
  - fulltext password always (basic authentication)

Downgrade attacks

- Most cryptographic protocols allow for some negotiation of cryptographic suites
  - RDP security layer without NLA
  - TLS renegotiation attack
  - Fallback to NTLM in HTTP/SMB/LDAP/DCOM etc.
- MITM attacker may force either party to unencrypted channel
  - TLS Strip attack (proxy HTTP 301/302)

Cryptographic algorithms

- Hash algorithms
  - no keys
- Symmetric key algorithms
  - secret key
- Asymmetric key algorithms
  - encryption and decryption key
  - public and private key

Safe algorithm comparison

Algo	Use	Notes
AES	symmetric encryption	
SHA2	hashing	
RSA 2048+	asymmetric encryption/signature/key generation	
ECDH	asymmetric key generation	
ECDSA	asymmetric encryption/signature	Incompatible today

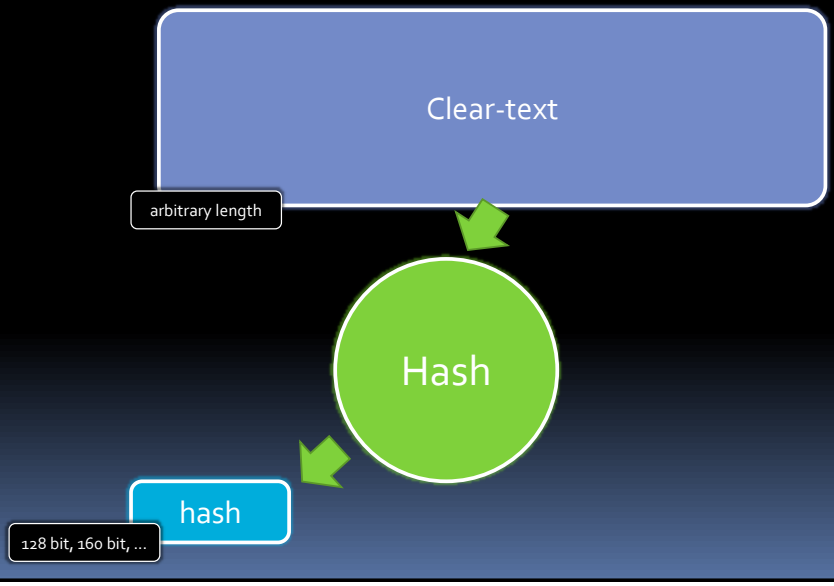
Combinations possible everywhere since Windows 7 and Windows 2008 R2
AES + SHA2 + RSA signature + RSA key generation
AES + SHA2 + RSA signature + ECDH key generation

Combinations possible somewhere since Windows 7 and Windows 2008 R2
AES + SHA2 + ECDSA signature + ECDH key generation

Enterprise PKI

HASH ALGORITHMS

Hashing



Algorithm examples

- MD2, MD4, MD5
- SHA-1
  - 160 bit, original security 2^128, now 2^60
- SHA2 (SHA-256, SHA-384, SHA-512)

Hash

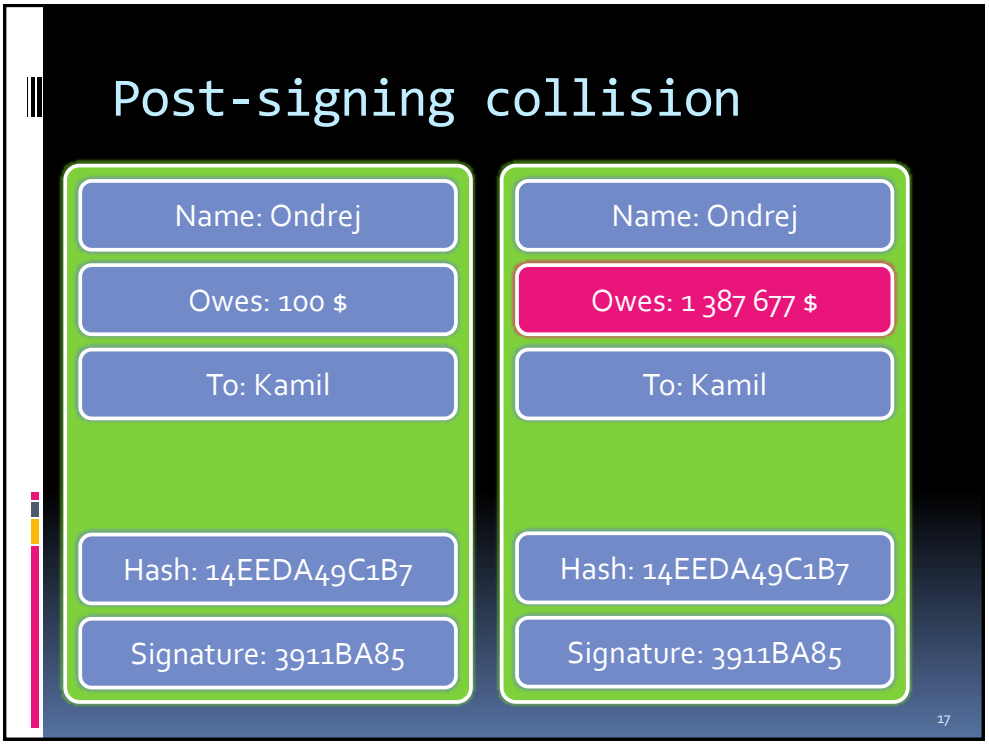
- Data authentication and integrity
  - in conjunction with keys
  - HMAC – Hashed Message Authentication Code
- Compression of messages for digital signatures
- Deriving keys
- Generation of deterministic random numbers

Incorrect hash example

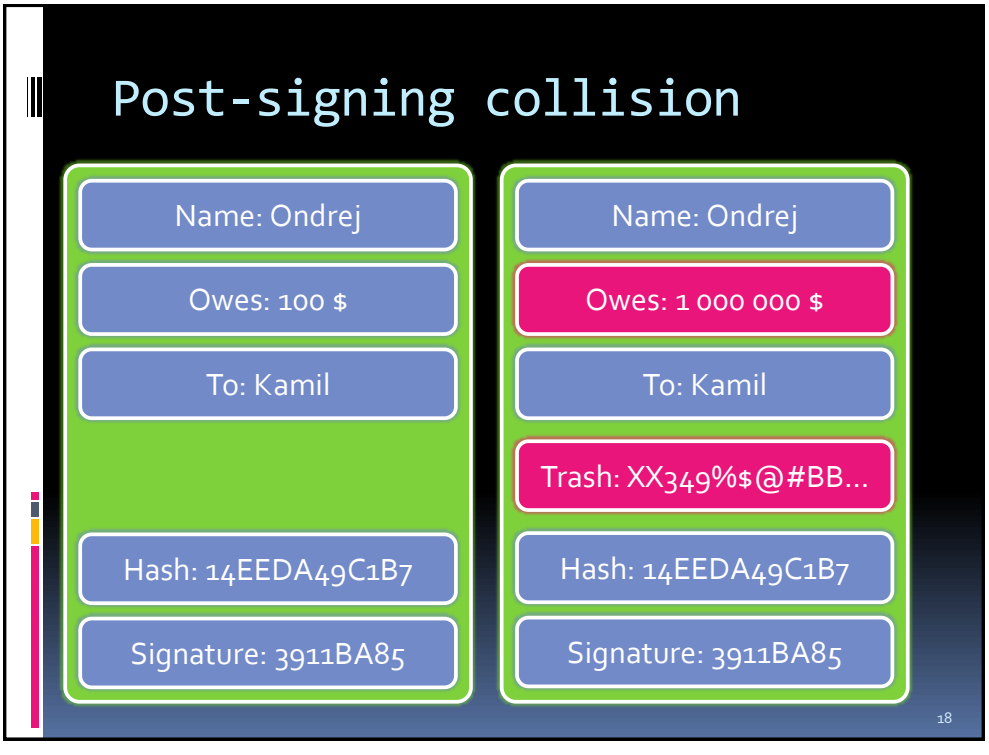
- Sum alphabet letter positions
  HELLO = 8 + 5 + 12 + 12 + 15 = 52
- Can obtain arbitrary clear-text (collision) without brute-forcing
- Two similar clear-texts lead to similar output

Hash collisions

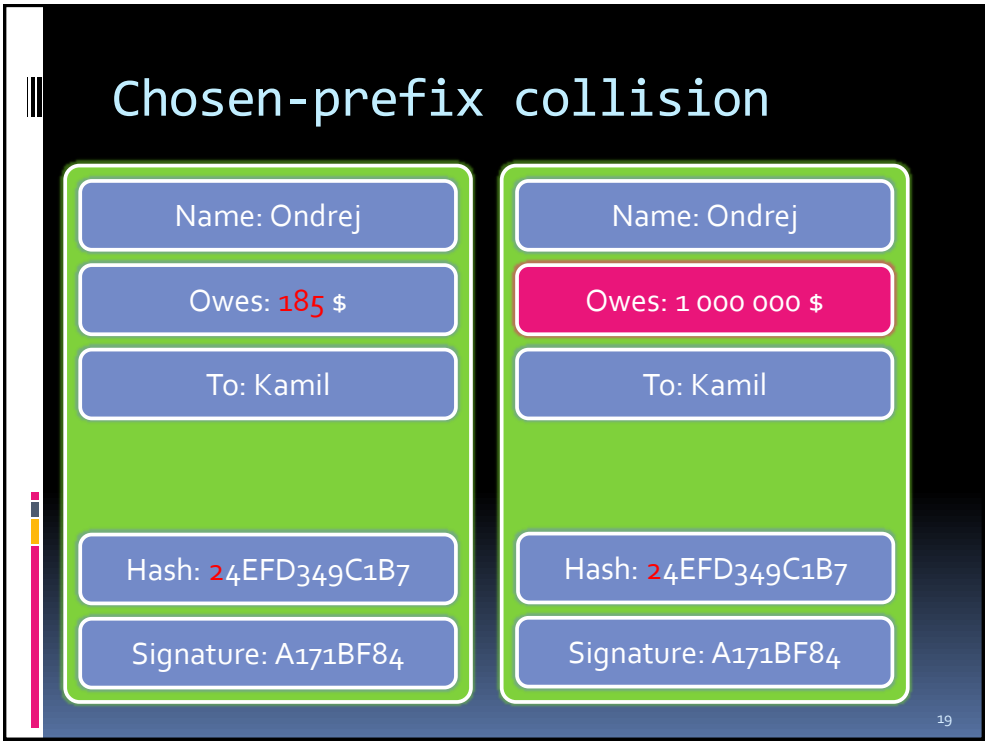
- Pure arithmetic collisions
  - limited exploitability
- Post-signing collisions
  - the best to have
- Chosen-prefix (pre-image) collisions
  - some pre-known hash values grant better collions


Post-signing collision
Name: Ondrej
Owes: 100 $
To: Kamil
Hash: 14EEDA49C1B7
Signature: 3911BA85
Name: Ondrej
Owes: 1 387 677 $
To: Kamil
Hash: 14EEDA49C1B7
Signature: 3911BA85
17

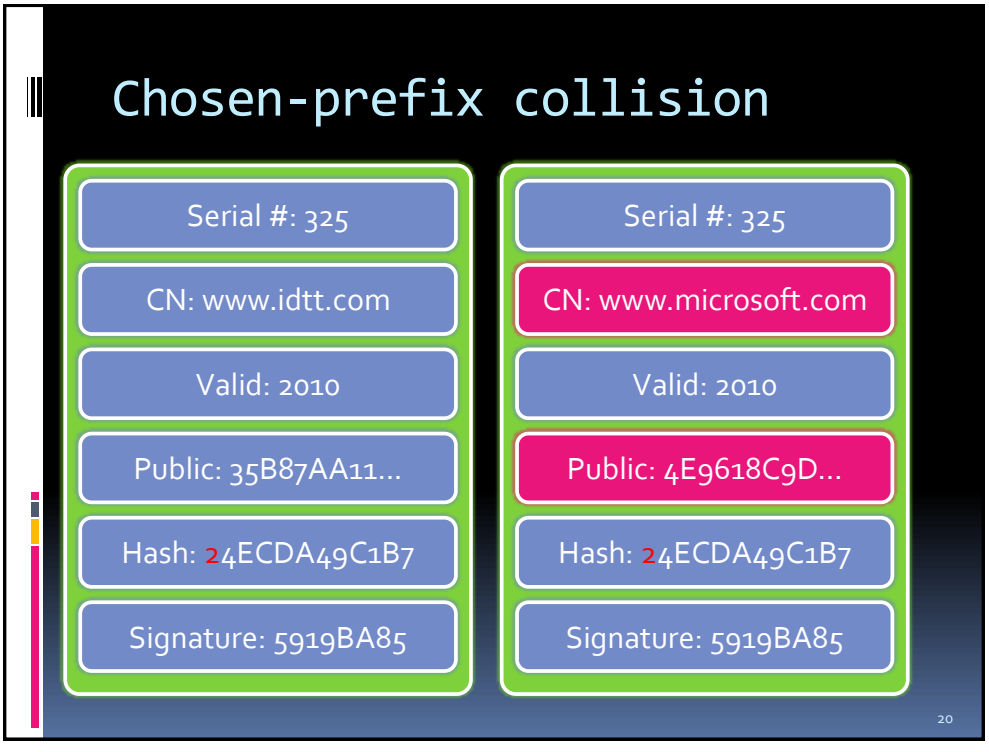
17


Post-signing collision
Name: Ondrej
Owes: 100 $
To: Kamil
Hash: 14EEDA49C1B7
Signature: 3911BA85
Name: Ondrej
Owes: 1 000 000 $
To: Kamil
Trash: XX349%$@#BB...
Hash: 14EEDA49C1B7
Signature: 3911BA85
18

18


Chosen-prefix collision
Name: Ondrej
Owes: 185 $
To: Kamil
Hash: 24EFD349C1B7
Signature: A171BF84
Name: Ondrej
Owes: 1 000 000 $
To: Kamil
Hash: 24EFD349C1B7
Signature: A171BF84
19

19


Chosen-prefix collision
Serial #: 325
CN: www.idtt.com
Valid: 2010
Public: 35B87AA11…
Hash: 24ECDA49C1B7
Signature: 5919BA85
Serial #: 325
CN: www.microsoft.com
Valid: 2010
Public: 4E9618C9D…
Hash: 24ECDA49C1B7
Signature: 5919BA85
20

20

MD5 problems

- Pure arithmetic in 2^112 evaluations
- Post-signing collisions suspected
- Chosen-prefix collisions
  - Practically proved for certificates with predictable serial numbers
  - 2^50

SHA-1 problems

- General brute-force attack at 2^60
  - as about 12 characters complex password

Windows passwords

- MD4
  - 10x faster than SHA-1
- Can be captured from
  - Active Directory or local account databases
  - local password cache
  - from LSASS memory
  - in transmit from NTLM, Kerberos
  - on network services from NTLM

Windows passwords

- 8 characters password?
- 80^8 possible passwords
- 2^x = 80^8 ??
  - x * log 2 = 8 * log 80
  - x = 8 * log 80 / log 2
  - x ~= 51
- 10 characters ~= 2^63
- 12 characters ~= 2^76

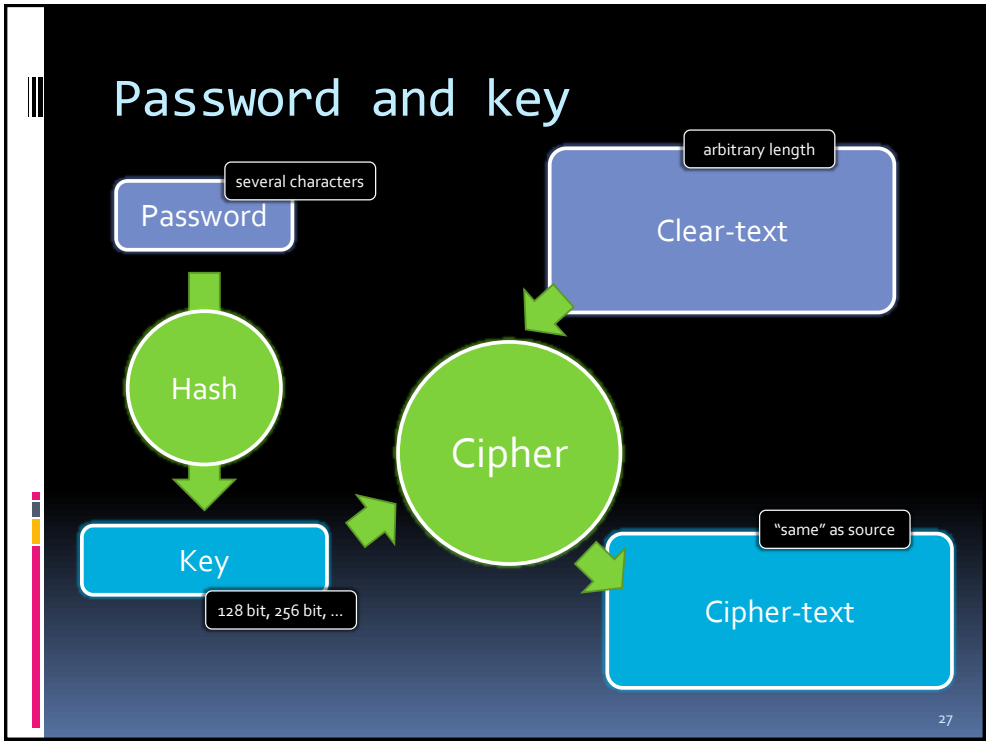
Enterprise PKI

SYMMETRIC ALGORITHMS

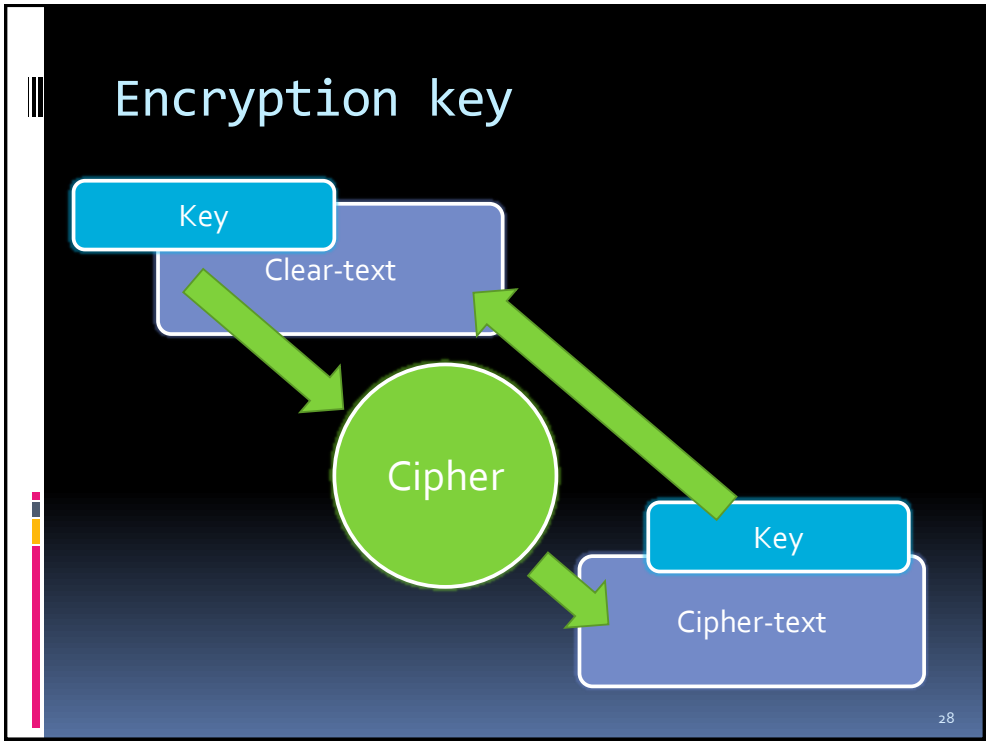
Symmetric key

- Data confidentiality
- Authentication and integrity
  - MAC – Message Authentication Code, single key to generate, the same to validate
- Key establishment
- Generation of deterministic random numbers

- RC4, DES, 3-DES (TDEA), AES


Password and key
several characters
Password
arbitrary length
Clear-text
Hash
Cipher
Key
128 bit, 256 bit, ...
"same" as source
Cipher-text
27

27


Encryption key
Key
Clear-text
Cipher
Key
Cipher-text
28

28

Enterprise PKI

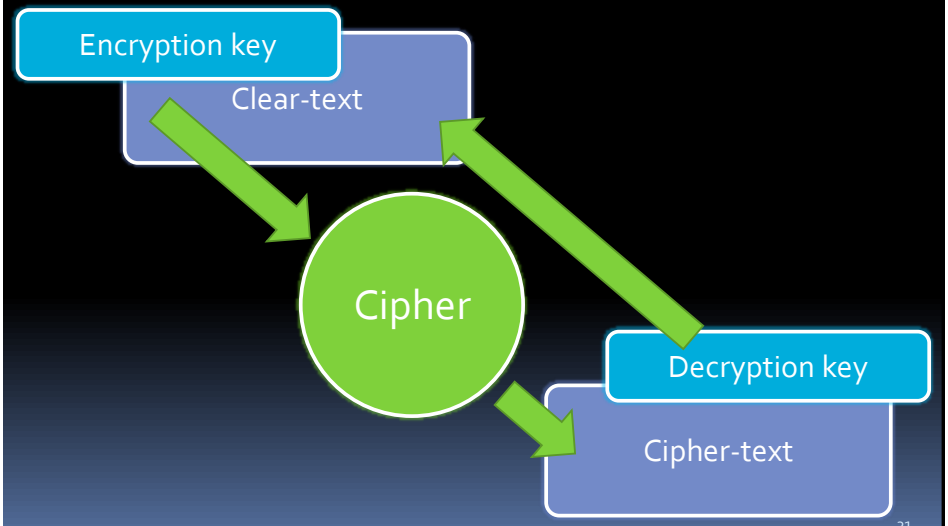
ASYMMETRIC ALGORITHMS

Asymmetric keys

- Digital signatures
- Key establishment
- Generation of random numbers

- RSA, DSA, ECDSA
- RSA Key Exchange, Diffie-Hellman (DH), ECDH

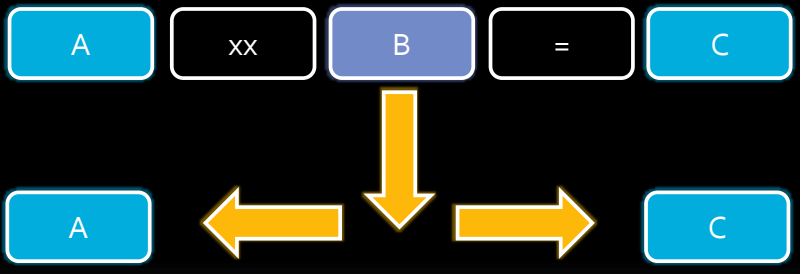
Encryption and decryption keys



31

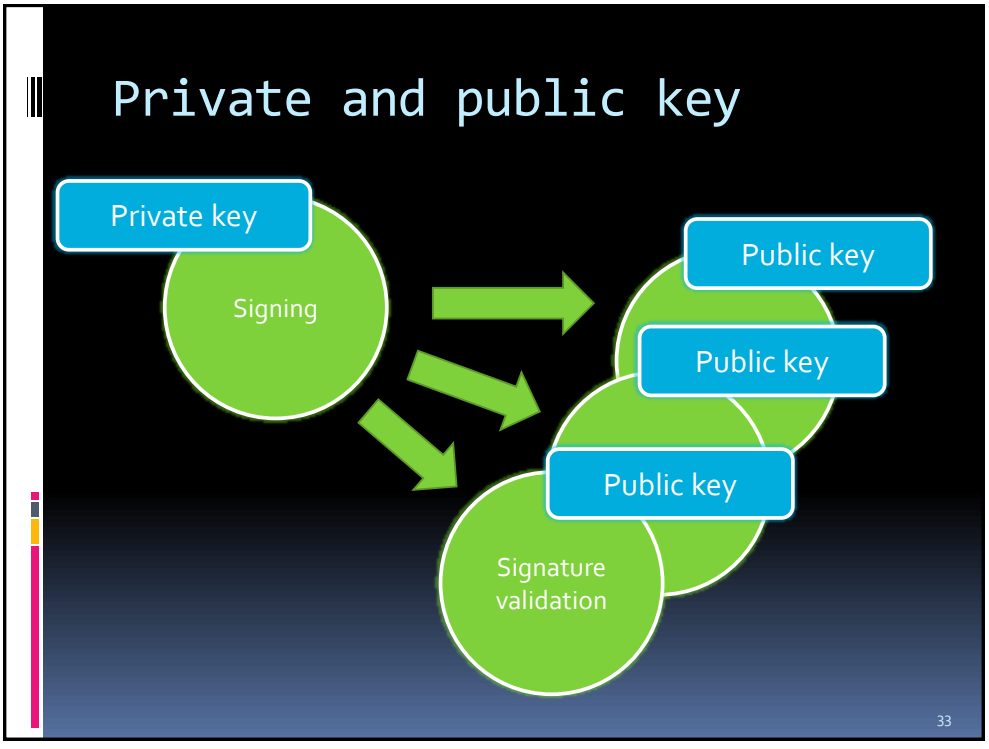
31

Key derivation

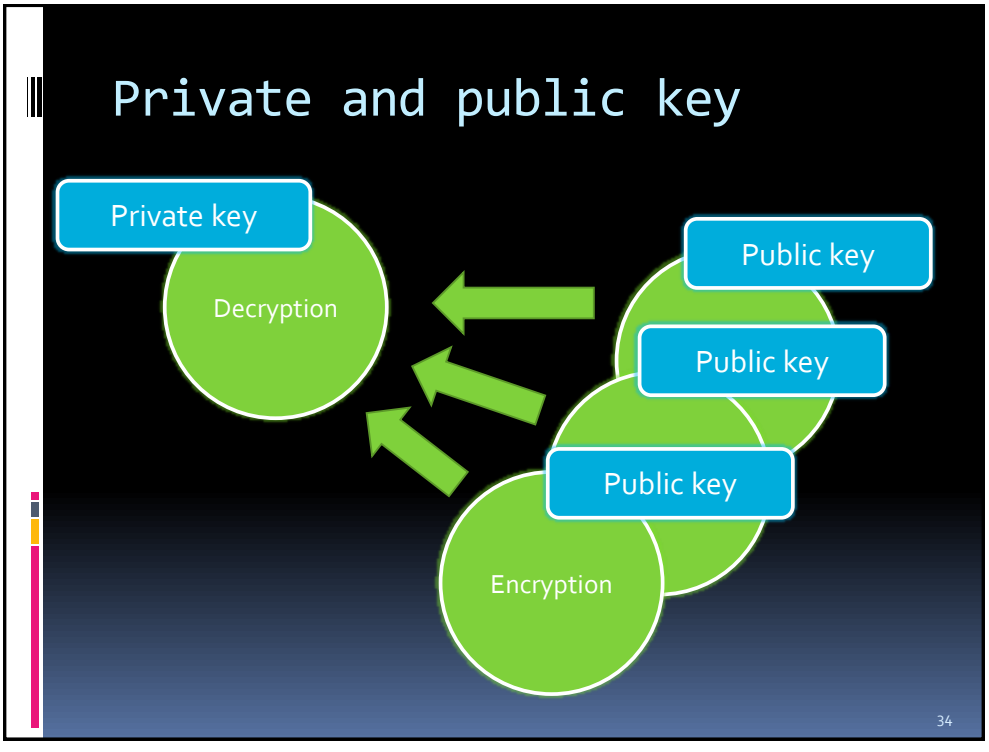


DSA, RSA – mod (primeA * primeB)
DH – primeA mod primeB
ECxx – x^primeA + y^primeB

32


Private and public key
Private key
Signing
Public key
Public key
Public key
Signature validation
33

33

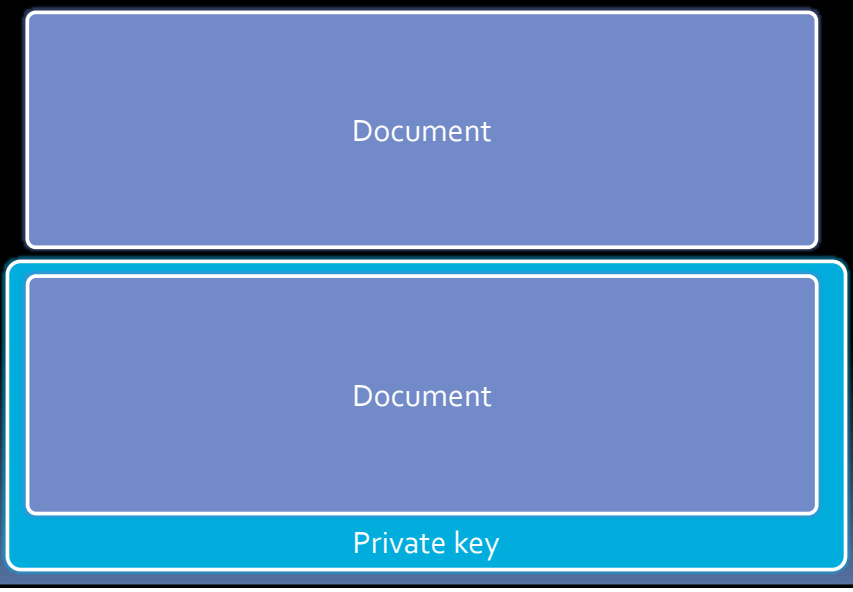

Private and public key
Private key
Decryption
Public key
Public key
Public key
Encryption
34

34

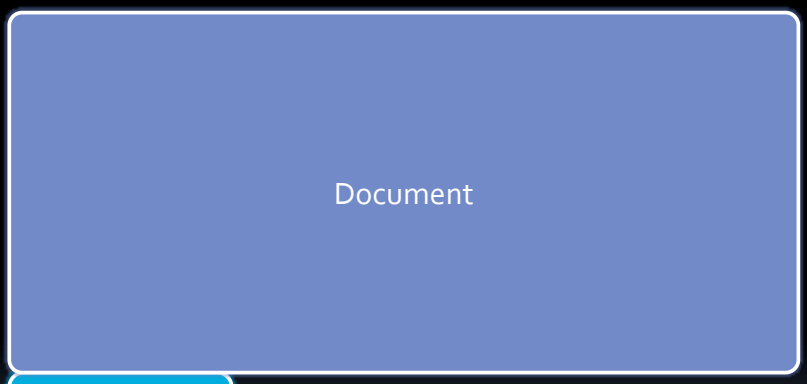
Performance considerations

- Asymmetric algorithms use large keys
  - EC is about 10 times smaller
- Encryption/decryption time about 100x longer
  - symmetric is faster
- 2x longer keys
  - 16x longer time for key preparation
  - 8x longer private key operations
  - 4x longer public key operations

Digital signature (incorect)

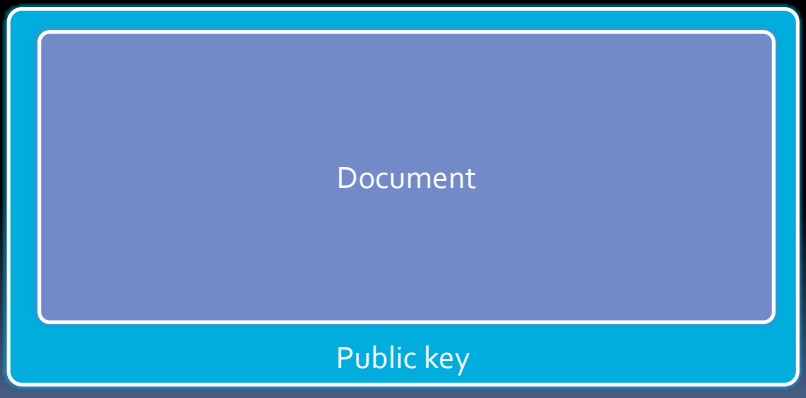


Digital signature

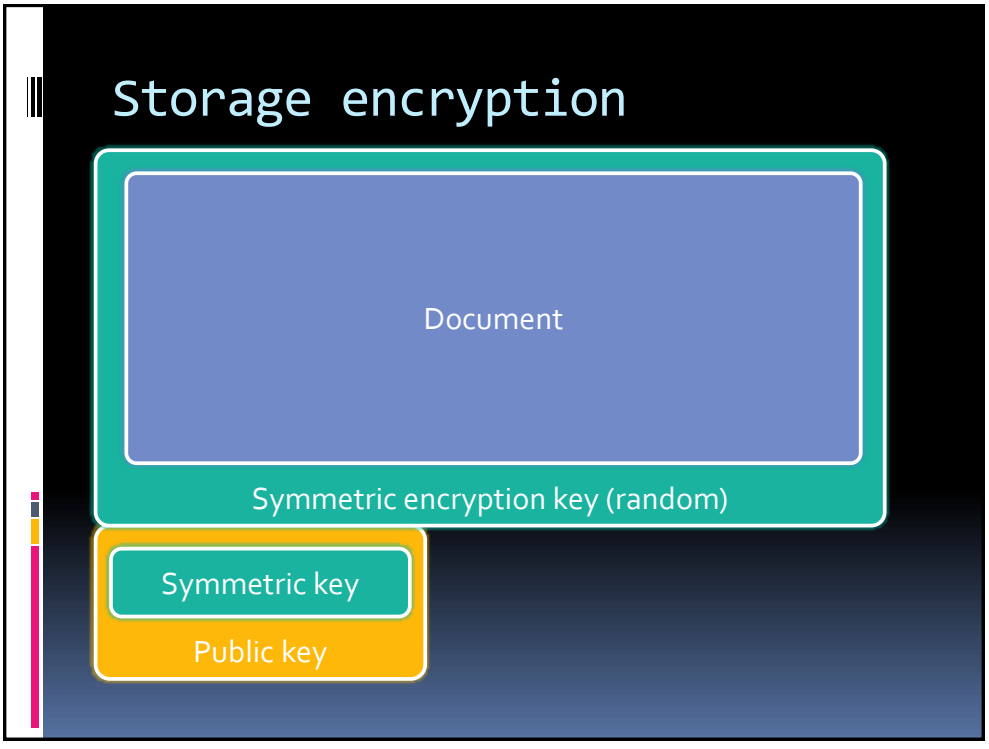


37

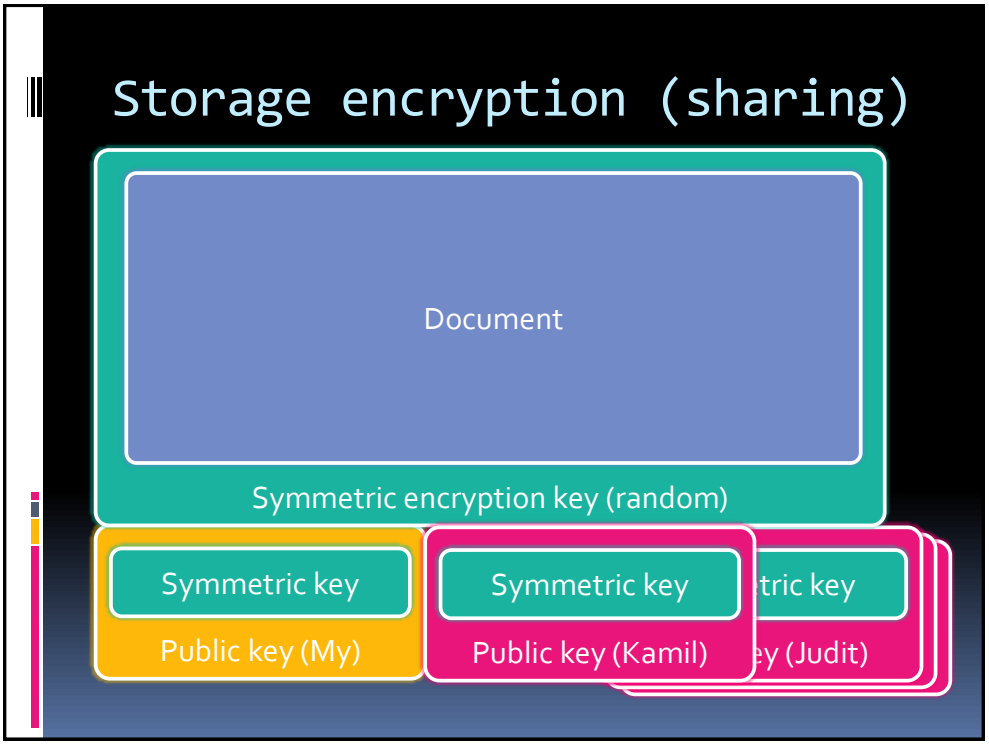
Storage encryption (slow, with more users excessive mail traffic/storage)



38

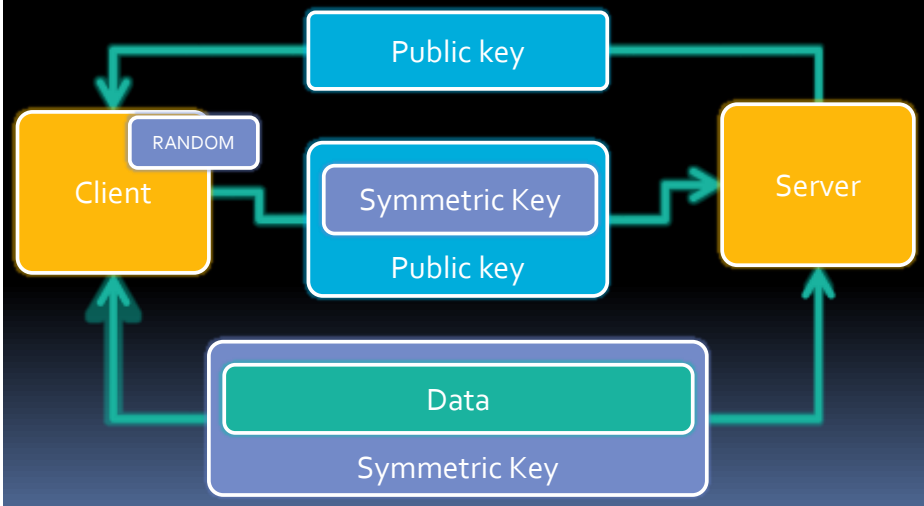

Storage encryption
Document
Symmetric encryption key (random)
Symmetric key
Public key

39


Storage encryption (sharing)
Document
Symmetric encryption key (random)
Symmetric key
Public key (My)
Symmetric key
Public key (Kamil)
tric key
y (Judit)

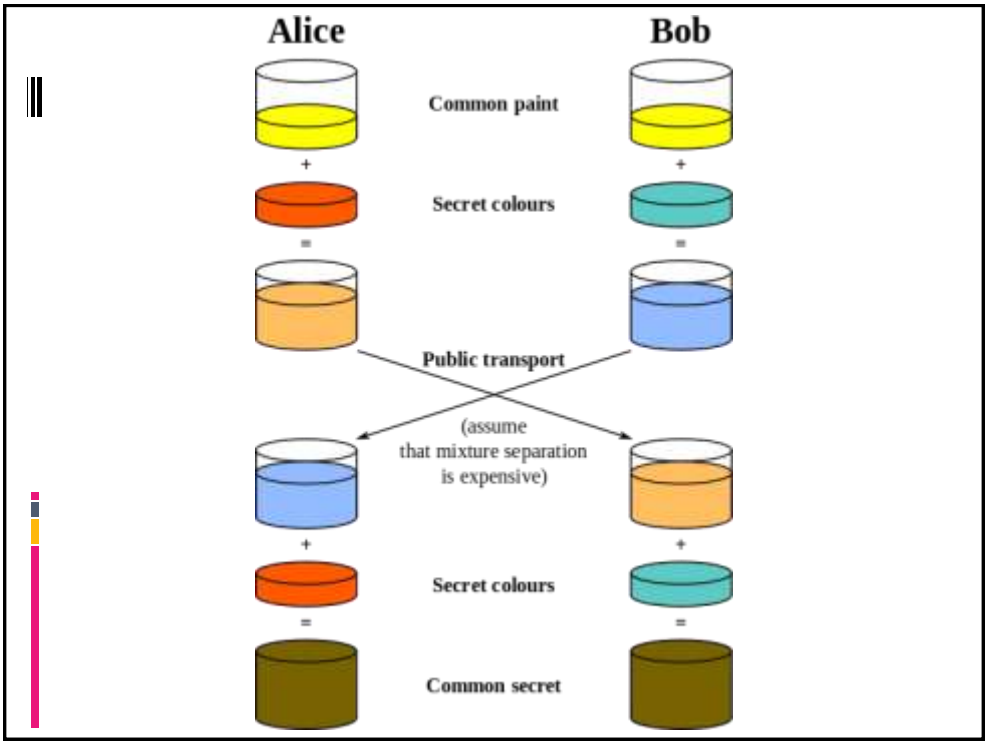
40

Transport encryption with key encipherment

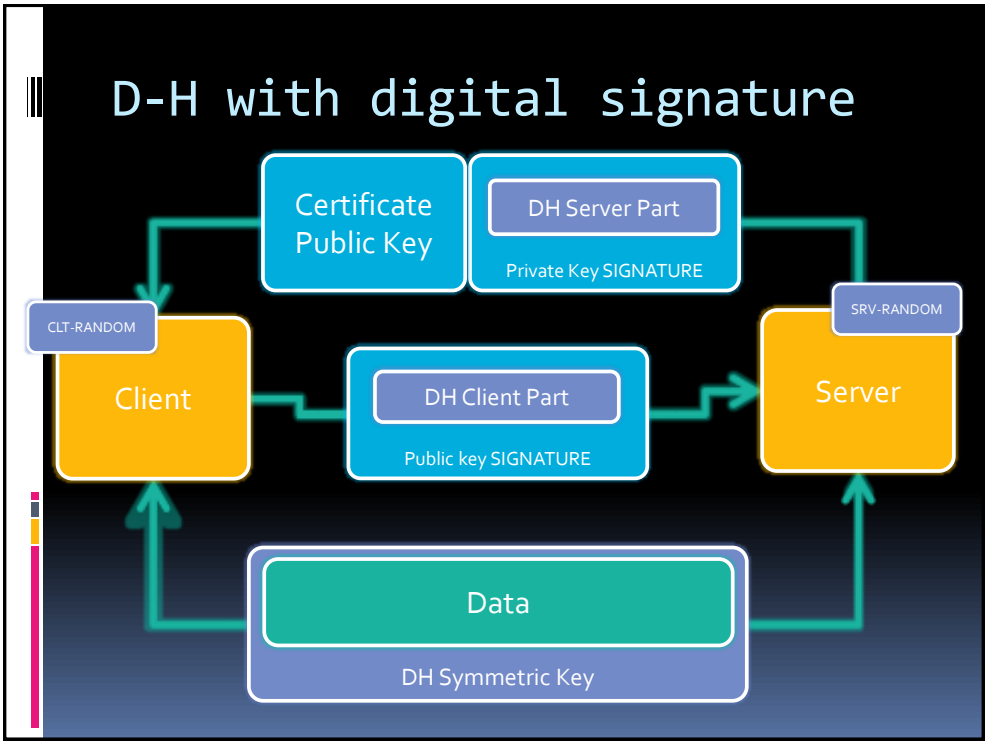


Diffie-Hellman key agreement

- Asymmetric algorithm for symmetric key exchange
  - most commonly used for key exchange
- Automatically generates the same encryption key for symmetric encryption on both sides


Alice
Bob
Common paint
Secret colours
Public transport
(assume
that mixture separation
is expensive)
Secret colours
Common secret

43


D-H with digital signature
Certificate
Public Key
DH Server Part
Private Key SIGNATURE
CLT-RANDOM
Client
DH Client Part
Public key SIGNATURE
SRV-RANDOM
Server
Data
DH Symmetric Key

44

Key Exchange vs. Key Agreement

- RSA key exchange
  - server sends public key to the client
  - client generates random symmetric key
  - srvPublic(randomSym)
  - Key Usage: Key Encipherment
- Diffie-Hellman key agreement
  - server generates random D-H key part
  - srvPrivate(randomDH)
  - Key Usage: Digital Signature

Example algorithm combinations

Identity signature: RSA + SHA1 Key Exchange: RSA KE Data Encryption: AES Data integrity: SHA256	Identity signature: RSA + MD5 Key Exchange: RSA KE Data Encryption: 3DES Data integrity: SHA-1
Identity signature: ECDSA + SHA-256 Key Exchange: ECDH KA Data Encryption: AES Data integrity: MD5	Identity signature: DSA + SHA1 Key Exchange: DH KA Data Encryption: 3DES Data integrity: SHA256

Perfect Forward Secrecy (PFS)

- RSA key exchange
  - keys encrypted with long-term private key
  - later private key disclosure allows data decryption
- (EC)DH key agreement
  - keys only signed
  - later private key disclosure is safe

Enterprise PKI

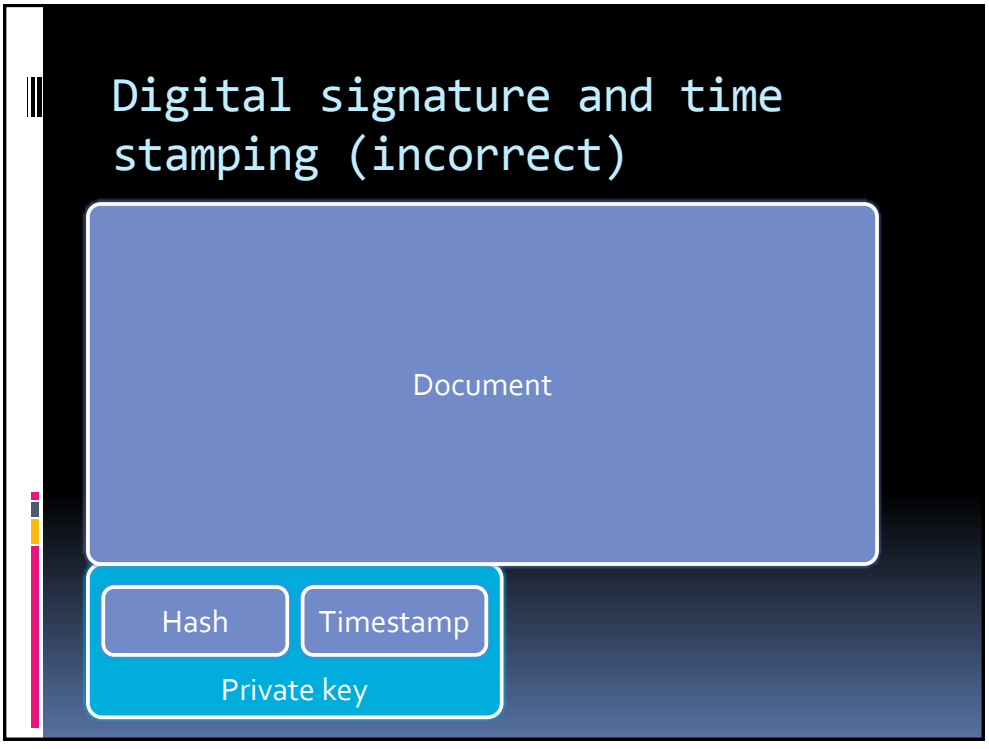
TIME STAMPS

Timestamping vs. signatures

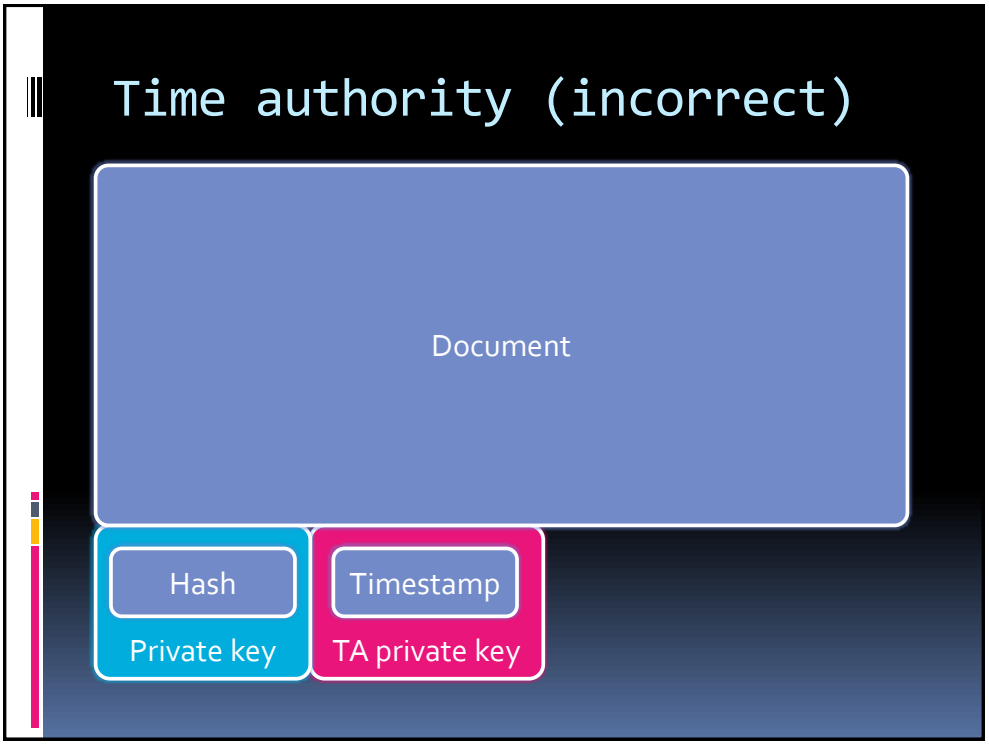
- Signature
  - proves identity of an author or "agreeer"
  - an invoice is signed by the seller to manifest his consent with a trade agreement
- Timestamp
  - confirms possession of data before the point in time
  - buyer timestamps all received invoices to be able to prove their timely possession to tax authorities

Reason for timestamps

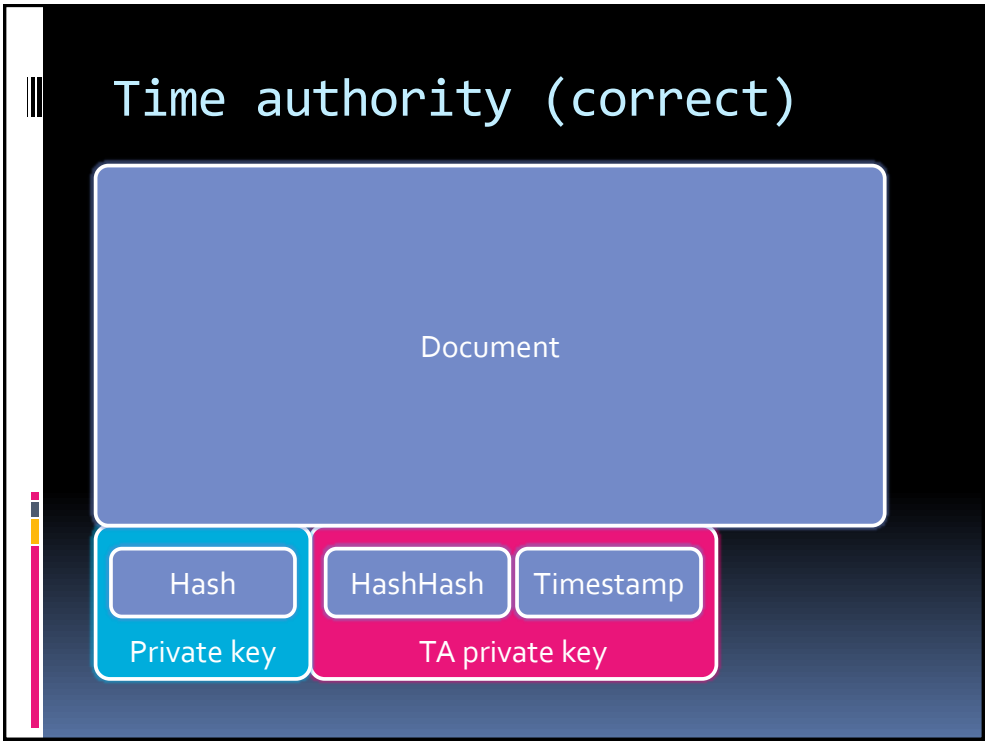
- Subject of a digital certificate is responsible for security of its private key only during the validity of the certificate
  - After the certificate expires, anybody may obtain its private key and sign whatever retrospectively
- Evidence responsibility lies at the recipient of a digital signature
  - not the signer


Digital signature and time stamping (incorrect)
Document
Hash
Timestamp
Private key

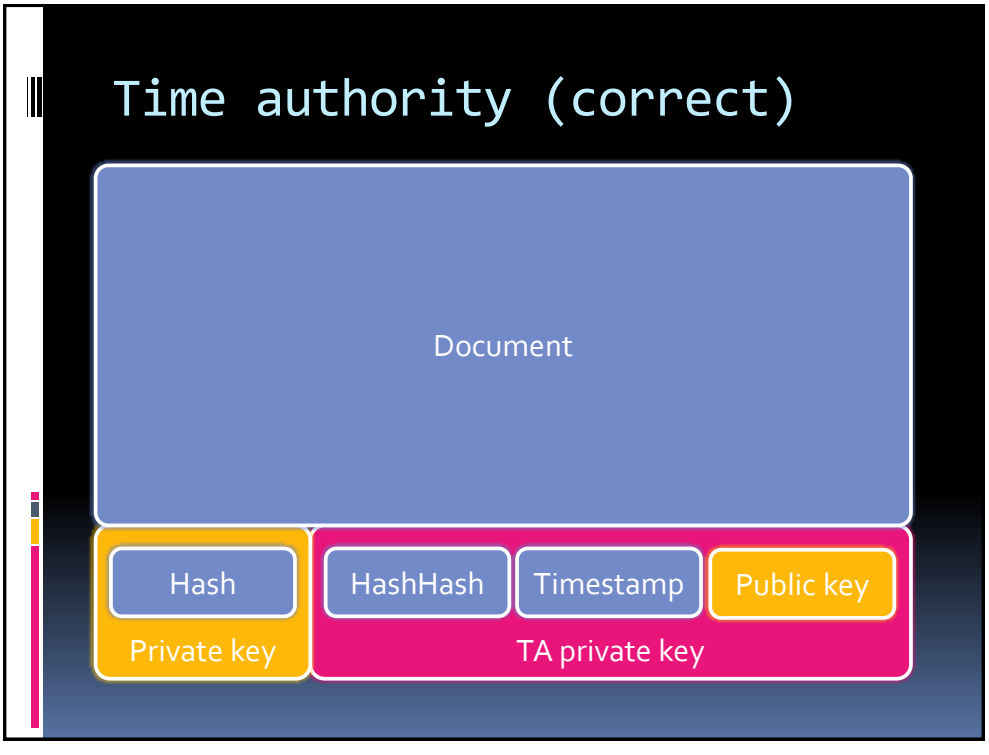
51


Time authority (incorrect)
Document
Hash
Private key
Timestamp
TA private key

52


Time authority (correct)
Document
Hash
Private key
HashHash
Timestamp
TA private key

53


Time authority (correct)
Document
Hash
Private key
HashHash
Timestamp
Public key
TA private key

54

Standards

- RFC 3161 - Timestamp Protocol (TSP)
  - http://timestamp.globalsign.com/scripts/timstamp.dll
  - https://timestamp.geotrust.com/tsa
  - http://timestamp.digicert.com
  - http://timestamp.apple.com/ts01

Enterprise PKI

RANDOM NUMBERS

Random number generators

- Deterministic RNG use cryptographic algorithms and keys to generate random bits
  - attack on randomly generated symmetric keys
  - DNS cache poisoning
- Nondeterministic RNG (true RNG) use physical source that is outside human control
  - smart cards, tokens, TPM
  - HSM – hardware security modules

Random number generators

- Win32API: CryptGenRandom()
  C#: RNGCryptoServiceProvider
  - hashed
  - Vista+ AES (NIST 800-90A)
  - 2003- DSS (FIPS 186-2)
- Entropy from
  - system time, process id, thread id, tick counter, virtual/physical memory performance counters of the process and system, free disk clusters, user environment, context switches, exception count, ...

Random number generators

- new Random()
  - just a time seed
  - several instances created simultaneously may have the same seed

Dual_EC_PRNG controversy (Dual_EC_DRBG)

- NIST SP800-90
  - pressed into the standard by NSA
- possible back-door
- 1000x slower than others
- some "random contants" that may have "secret counterparts"
  - if somebody knows them, he can predict the random results
- removed 2014, P-256 suspected => X25519, X448

Enterprise PKI

SMART CARDS AND HSM

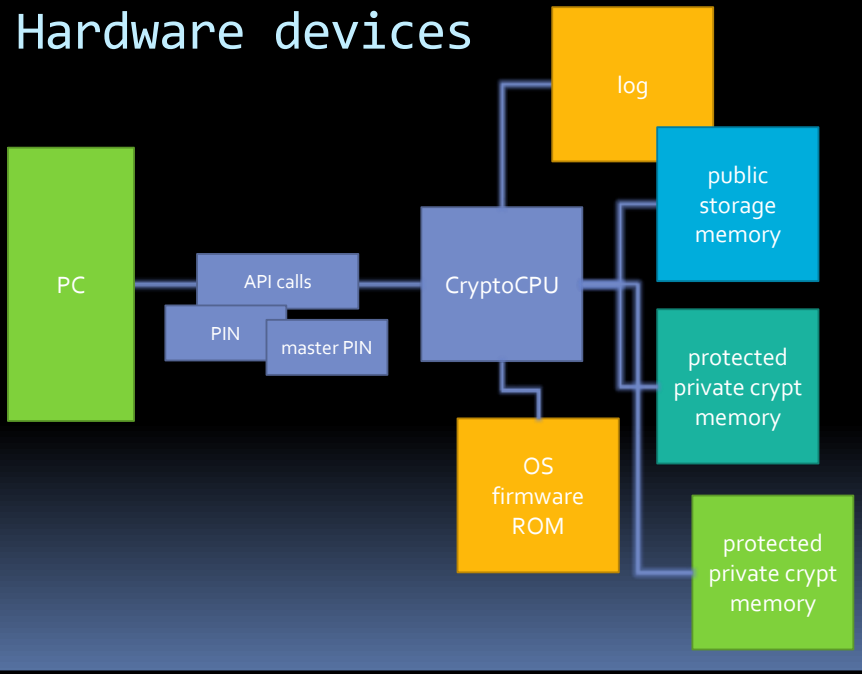
Cryptographic devices

- Smart cards and tokens, TPM
  - cryptoCPU
  - safe memory for storing private information
  - flash memory for public data
- Hardware security modules (HSM)
  - bigger smart cards
  - self powered, fire protected, temper proof
  - connected over network or USB etc.

Cryptographic devices security

- Can generate hardware randoms
- Generate-only or write-only private keys
- User PIN
  - perform crypto operations with private keys only
- Master PIN
  - manage keys, export, import, delete, …
  - not always available

Hardware devices



Hardware supported offloading

- AES-NI
  - Some newer Intel and AMD processors since 2008
  - Supported by CNG providers since Windows 7
- RSA offloading
  - PCI card + software SChannel plug-in

65

Enterprise PKI

CURRENT ALGORITHMS

66

66

Symmetric algorithm history

- DES (1976, 56 bit)
- 3DES, TDEA (1998, 168/112 bit)
- RC4 (1987, 128 bit)
- AES-128, AES-192, AES-256 (2001)

Hash algorithm history

- MD4 (1990, 128 bit)
- MD5 (1991, 128 bit)
- SHA-1 (1995, 160 bit)
- SHA-224, SHA-256, SHA-384, SHA-512 (2001)

Asymmetric algorithm history

- RSA (1973)
- DSA (1991)
- ECDSA (2000)
- ECDH (2000)

Enterprise PKI

CRYPTOGRAPHIC STANDARDS

US standards

- FIPS – Federal Information Processing Standards
  - provides standard algorithms
- NIST – National Institute for Standards and Technology
  - approves the algorithms for US government non-classified but sensitive use
  - latest NIST SP800-57, March 2007
- NSA – National Security Agency
  - Suite-B for Secure and Top Secure (2005)

Hash functions (SP800-57)

- SHA-1
  - hash size output is 160
- SHA2
  - SHA-224, SHA-256, SHA-384, SHA-512
  - hash size output is 224, 256, 384, 512

Symmetric key (SP800-57)

- AES-128, AES-192, AES-256
  - encrypts data in 128-bit blocks
  - uses 128, 192, 256-bit keys
- Triple DEA (TDEA)
  - encrypts data in 64-bit blocks
  - uses three 56-bit keys

Digital Signatures (SP800-57)

- DSA (Digital Signature Algorithm)
  - key sizes of 1024, 2048 and 3072-bit
  - produces 320, 448, 512-bit signatures
- RSA (Rivest – Shamir – Adleman)
  - key sizes according to FIPS186-3
  - must be PKCS #1 2.1
- ECDSA (Elliptic Curve DSA)
  - key sizes of at least 160-bit
  - produces 2x key length signatures
  - types of curves specified in FIPS186-3

What is not a FIPS algorithm

- MDx
- RC4
- SSL (but TLS is)

- NTLMv2 is HMAC-MD5
- Kerberos uses RC4 by default
- WEP uses RC4
- MPPE uses RC4
- WPA TKIP is RC4
- WPA CCMP is AES

Crypto-periods (SP800-57)

Key	Cryptoperiod
Private signature	1 – 3 years
Public signature verification	>3 years
Symmetric authentication	<= 5 years
Private authentication	1-2 years
Symmetric data encryption	<= 5 years
Public key transport key	1-2 years
Private/public key agreement key	1-2 years

Comparable Algorithm Strengths (SP800-57)

Strength	Symmetric	RSA	ECDSA ECDH	SHA	nonFIPS
80 bit	2TDEA	RSA 1024	ECDSA 160 ECDH 160	SHA-1	
112 bit	3TDEA	RSA 2048	ECDSA 224 ECDH 224	SHA-224	MD5
128 bit	AES-128	RSA 3072	ECDSA 256 ECDH 256	SHA-256	RC4
192 bit	AES-192	RSA 7680	ECDSA 384 ECDH 384	SHA-384	
256 bit	AES-256	RSA 15360	ECDSA 521 ECDH 521	SHA-512	

77

Security lifetimes (SP800-57 and Suite-B)

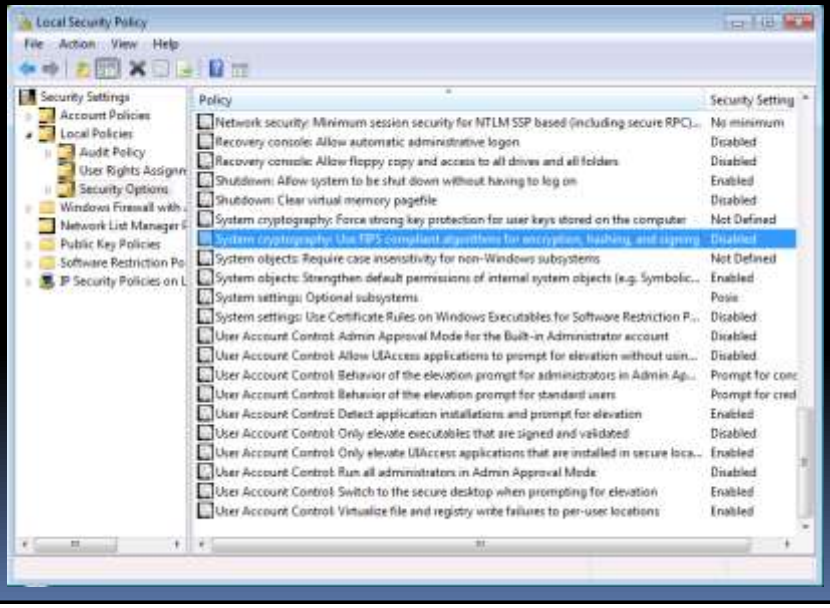
Lifetime	Strength	Level
2010	80 bit	US Confidential
2030	112 bit	US Confidential
	128 bit	US Secure
	192 bit	US Top-Secure
Beyond 2030	128 bit	US Confidential

78

Enterprise PKI

OPERATING SYSTEM SUPPORT

FIPS Compliant Algorithms



FIPS Compliant Algorithms

- Disables SSL 2.0 and SSL 3.0
- Allows only TLS 1.0
  - RDP supported since Windows 2003 SP1
  - RDP client 5.2+
- Cannot do RC4
- Cannot do MD5

Cryptographic providers (CryptoAPI)

- Cryptographic Service Provider – CSP
  - Windows 2000+
  - RSA, DSS/DSA, DH, (AES), (SHA2)
- Cryptography Next Generation – CNG, KSP (Key Storage Provider)
  - Windows Vista+/2008+
  - RSA, DSS/DSA, DH, AES, SHA2, ECDSA, ECDH
  - CNG Key Isolation service according to CC
- CERTUTIL -CSPLIST

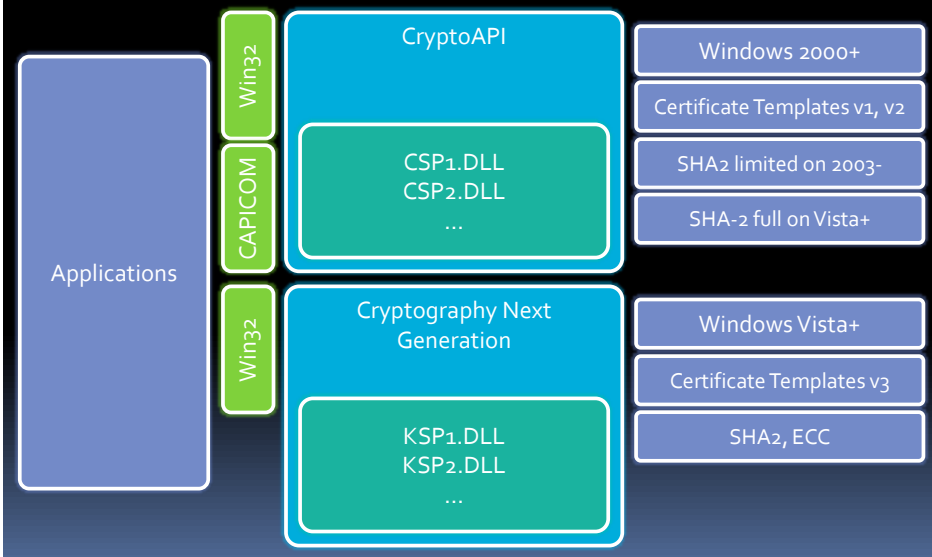
Hardware providers

- Cryptographic Service Provider – CSP
  - Schlumberger (2000, XP, 2003)
  - SafeSign
  - CryptoPlus
  - Microsoft Base Smart Card Crypto Provider
    - plus minidriver for each smart card
- Cryptography Next Generation – CNG/KSP
  - Microsoft Smart Card Key Storage Provider

CSP Algorithms

- CryptoAPI Cryptographic Service Provider
  - http://msdn.microsoft.com/en-us/library/windows/desktop/bb931357(v=vs.85).aspx
- SHA256
  - Base Smart Card Crypto Provider
  - Microsoft Enhanced RSA and AES Cryptographic Provider
  - Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)

CSP vs. CNG



CSP and algorithms

Name	Type	Algo
Microsoft DSS Cryptographic Provider	PROV_DSS	DSS signature no DH
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider	PROV_DSS_DH	DSS signature DH
Microsoft DSS and Diffie-Hellman/Schannel Cryptographic Provider	PROV_DH_SCHANNEL	DSS signature DH
Microsoft RSA/Schannel Cryptographic Provider	PROV_RSA_SCHANNEL	RSA exchange no DH
Microsoft Base Cryptographic Provider Microsoft Strong Cryptographic Provider Microsoft Enhanced Cryptographic Provider	PROV_RSA_FULL	RSA signature/exchange no DH
Microsoft AES Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider	PROV_RSA_AES	RSA signature/exchange no DH

Cryptography support

System	DES 3DES RC2 RC4	AES 128 AES 192 AES 256	MD2 MD5 HMAC	SHA-1	SHA-256 SHA-384 SHA-512	ECDSA ECDH
Windows 2000	yes	no	yes	yes	no	no
Windows XP	yes	yes	yes	yes	yes verify only	no
Windows 2003	yes	yes	yes	yes	non-public update yes verify only	no
Windows Vista/2008	yes	yes	yes	yes	yes	yes
Windows 7/2008 R2	yes	yes	yes	yes	yes	yes

Cryptography support

System	DES 3DES RC2 RC4	AES 128 AES 192 AES 256	MD2 MD5 HMAC	SHA-1	SHA-256 SHA-384 SHA-512	ECDSA
Windows Mobile 6.5	yes	yes	yes	yes	no	no
Windows Mobile 7	yes	yes	yes	yes	yes	yes
TMG 2010 WAP, ADFS 2016				yes	yes	no
SCCM 2007				yes	no	no
SCCM 2016 SCOM 2012 R2				yes	yes	no
SQL Server 2016				yes	yes	no
iOS 3	yes	yes	yes	yes	yes	no
iOS 5	yes	yes	yes	yes	yes	yes

Encryption

	EFS	BitLocker	IPSec	Kerberos	NTLM	RDP
DES	2000 +		2000 +	2000 +	LM password hash, NTLM	
3DES	2000 +		2000 +			2000 +
RC4				2000 +		2000 +
AES	2003 +	Vista +	Vista +	Vista +		
DH			2000 +			2000 +
RSA	2000 +	Seven +	2000 +	2000 +		2003 +
ECC	Seven +		Vista +	Seven +		

89

Hashing

	MD4	MD5	SHA-1	SHA2
NT password hash	NT4 +			
Digest password hash		2003 +		
IPSec		2000 +	2000 +	Seven +
NTLM		NTLMv2		
MS-CHAP		MS-CHAPv2		

90

90

SHA2 support

- CSPs can store and validate the SHA2 certificates
  - Windows XP SP3
  - Windows Server 2003 – KB 938397
  - Windows Mobile 7
- New SHA2 certificates can be issued only by Windows 2008+ CA
- Autoenrollment client can enroll for SHA2 certificates only on Windows 2008/Vista+
  - Windows XP SP3 + Server 2003 – KB 968730
- SHA256CryptoServiceProvider
  - .NET Framework 3.5 on Windows 2003 and newer, not supported on Windows XP

CNG support on templates

- Certificate Templates v1 and v2
  - always go into CSP
  - certificates will be SHA-1/SHA2 according to the CA-wide setting in the registry
- Templates v3
  - always go into CNG
  - cannot be re-imported into other CSPs (.PFX contains the original CSP name)
  - only for Windows Vista/2008+ clients
- Templates v4
  - go either into CSP or CNG
  - only for Windows 8/2012+ clients

CNG not supported

- EFS
  - Windows 2008/Vista-
  - user encryption certificates
- VPN/WiFi Client (EAPTLS, PEAP Client)
  - Windows 2008/7-
  - user or computer certificate authentication
- TMG 2010
  - server certificates on web listeners
- Outlook 2003
  - user email certificates for signatures or encryption
- Kerberos
  - Windows 2008/Vista- DC certificates
- System Center 2016/CurrentBranch-
- SQL Server 2016-
- Forefront Identity Manager 2010 (Certificate Management), Microsoft Identity Manager 2016
- AD FS and WAP on Windows 2016-
- RMS on Windows **2012** R2-

93

WS-SecurityPolicy 1.2

Algorithm Suite	[Dig]	[Enc]	[Sym KW]	[Asym KW]	[Enc KD]	[Sig KD]	[Min SKL]
Basic256	Sha1	Aes256	KwAes256	KwRsaOaep	PSha1L256	PSha1L192	256
Basic192	Sha1	Aes192	KwAes192	KwRsaOaep	PSha1L192	PSha1L192	192
Basic128	Sha1	Aes128	KwAes128	KwRsaOaep	PSha1L128	PSha1L128	128
TripleDes	Sha1	TripleDes	KwTripleDes	KwRsaOaep	PSha1L192	PSha1L192	192
Basic256Rsa15	Sha1	Aes256	KwAes256	KwRsa15	PSha1L256	PSha1L192	256
Basic192Rsa15	Sha1	Aes192	KwAes192	KwRsa15	PSha1L192	PSha1L192	192
Basic128Rsa15	Sha1	Aes128	KwAes128	KwRsa15	PSha1L128	PSha1L128	128
TripleDesRsa15	Sha1	TripleDes	KwTripleDes	KwRsa15	PSha1L192	PSha1L192	192
Basic256Sha256	Sha256	Aes256	KwAes256	KwRsaOaep	PSha1L256	PSha1L192	256
Basic192Sha256	Sha256	Aes192	KwAes192	KwRsaOaep	PSha1L192	PSha1L192	192
Basic128Sha256	Sha256	Aes128	KwAes128	KwRsaOaep	PSha1L128	PSha1L128	128
TripleDesSha256	Sha256	TripleDes	KwTripleDes	KwRsaOaep	PSha1L192	PSha1L192	192
Basic256Sha256Rsa15	Sha256	Aes256	KwAes256	KwRsa15	PSha1L256	PSha1L192	256
Basic192Sha256Rsa15	Sha256	Aes192	KwAes192	KwRsa15	PSha1L192	PSha1L192	192
Basic128Sha256Rsa15	Sha256	Aes128	KwAes128	KwRsa15	PSha1L128	PSha1L128	128
TripleDesSha256Rsa15	Sha256	TripleDes	KwTripleDes	KwRsa15	PSha1L192	PSha1L192	192

94

X509Certificate2

- .PrivateKey
- does not support CNG storage

95

Enterprise PKI

RSA COMPATIBILITY

96

Alternate signature formats for RSA

- Certificates contain OIDs that identify signatures
  - in case of RSA (not EC) it depends on PKCS #1 version
- PKCS #1 v1.5 (1993)
  - all Windows, combined OIDs
  - RSAMD5, RSASHA1, RSASHA256, …
- PKCS #1 v2.1 (2002)
  - Windows 2008/Vista+, separate OIDs
  - RSA, SHA1, SHA256, …

Alternate signature formats

- Certificate Template for requests
  - Use alternate signature format
- CA setting for issued certificates
  - CERTUTIL –setreg CA\CSP\AlternateSignatureAlgorithm 1

Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

THANK YOU!