Wireless Innovation Forum Webinar Series

Webinar #17: Review of WInnForum's COMSEC Document and Other Security Related Topics

9 February 2016

Thank You to Our Sponsors

FINMECCANICA

Google

MOTOROLA SOLUTIONS

THALES

Administrivia

Slides presented during this webinar will be posted here:

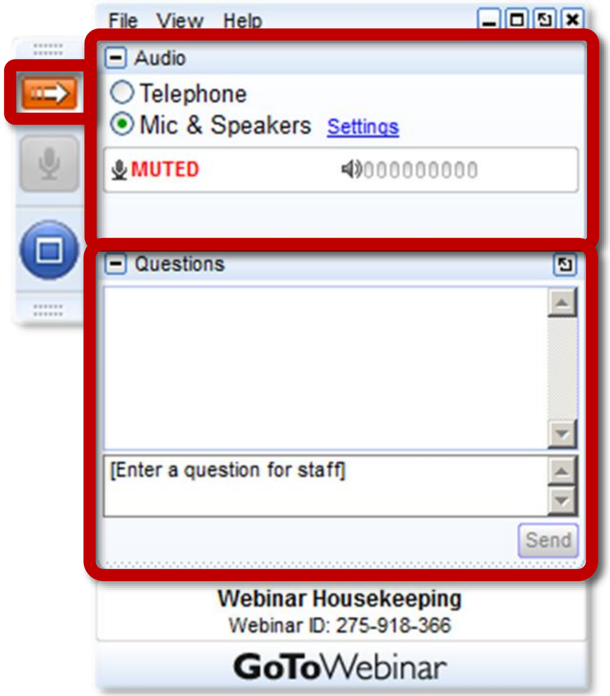
- http://www.wirelessinnovation.org/webinars

Email Lee.Pucker@wirelessinnovation.org if you need more information

Approved Reports, Recommendations and Specifications

- http://groups.winnforum.org/Forum_Work_Products

Go To Webinar Interface



Your Participation

Open and close your control panel

Join audio:

- Choose **Mic & Speakers** to use VoIP
- Choose **Telephone** and dial using the information provided

Submit questions and comments via the Questions panel

Note: Today’s presentation is being recorded and will be provided within 48 hours.

Driving the future of radio communications and systems worldwide

Today's Speakers

Greg Billock, Google

Matthew Probst, Federated Wireless

CBRS Security Webinar

9 February 2016

Cross-Working Group Security Webinar

Feb 9th, Noon to 2pm EST

1. PKI overview
2. Roles, Assets, & Trust Boundaries within CBRS
3. PKI Lifecycle/Usage for each trust role
   - Root:
   - Intermediate CAs
   - SAS
   - Domain Proxy
   - Professional Installers
   - PAL
   - CBSD
4. Summary
5. Q&A/Discussion

PKI Overview

"Alice and Bob" slides attributed to Jim Kurose and Keith Ross

12 Meanings of Security

Authentication*	Who am I talking to?
Authorization*	What should I be able to do?
Audit	Who did that?
Access control*	Should this request be honored?
Non-repudiation*	Can I pretend I never said that?
Confidentiality*	Can others see what I'm seeing?
Privacy*	Can others see that I'm seeing it?
Integrity*	Can this data be changed?
Anonymity*	Can others find out who I am?
Availability	Can I be assured of access when needed?
Durability	Will it be available in the future?
Physical security	Who can touch it?

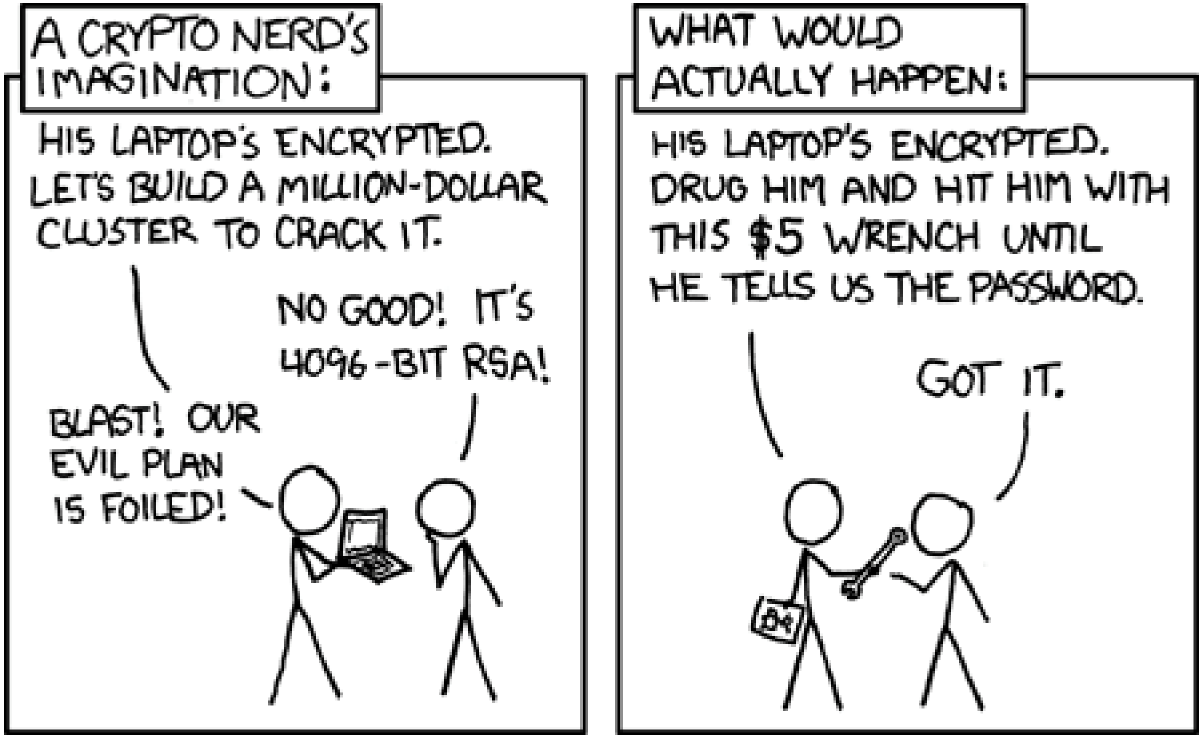
*Assisted by TLS + mutual certificate authentication

Credit: 11 from Alan Karp (HPL) … plus one

Know Limits of Cryptography

1) Establish policy *before* deciding how to to use Cryptography. Cryptography and PKI don't create policy. They can *help* enforce established policy.

2) Know Cryptography's limitations. Crypto must be complemented with other controls for full policy control:


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

Public Key Cryptography

symmetric key crypto

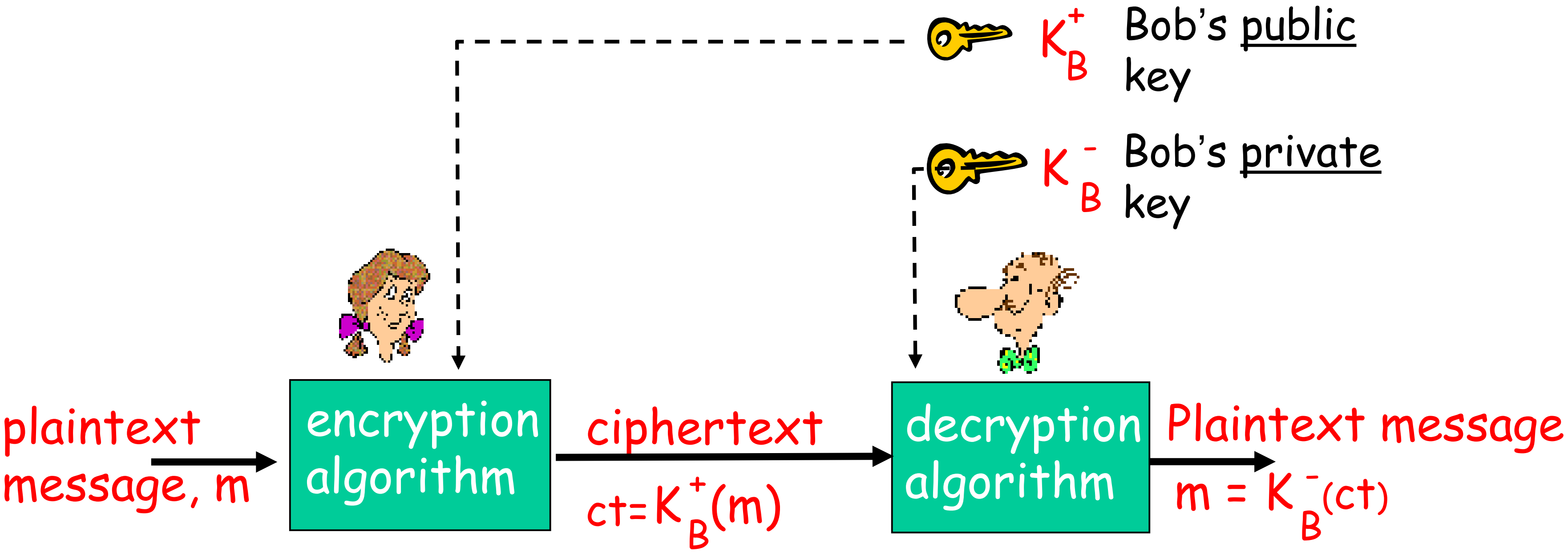
requires sender, receiver know shared secret key

Q: how to agree on key in first place (particularly if never "met")?

public key crypto

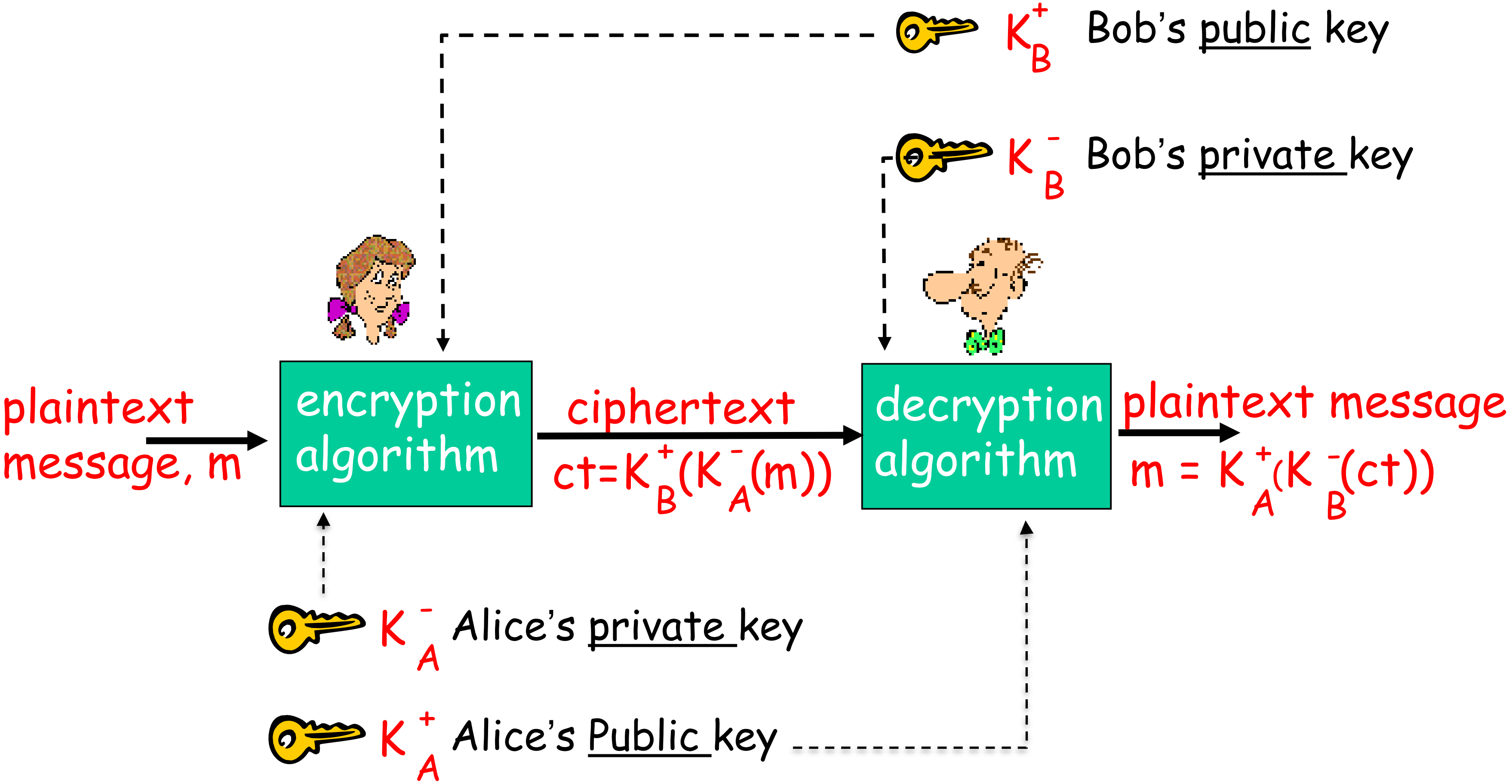
- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

Public key cryptography



Only Bob can read this message

Public key cryptography



K_B^+ Bob's public key

K_B^- Bob's private key

plaintext message, m

encryption algorithm

ciphertext

$ct=K_B^+(K_A^-(m))$

decryption algorithm

plaintext message

$m = K_A^+(K_B^-(ct))$

K_A^- Alice's private key

K_A^+ Alice's Public key

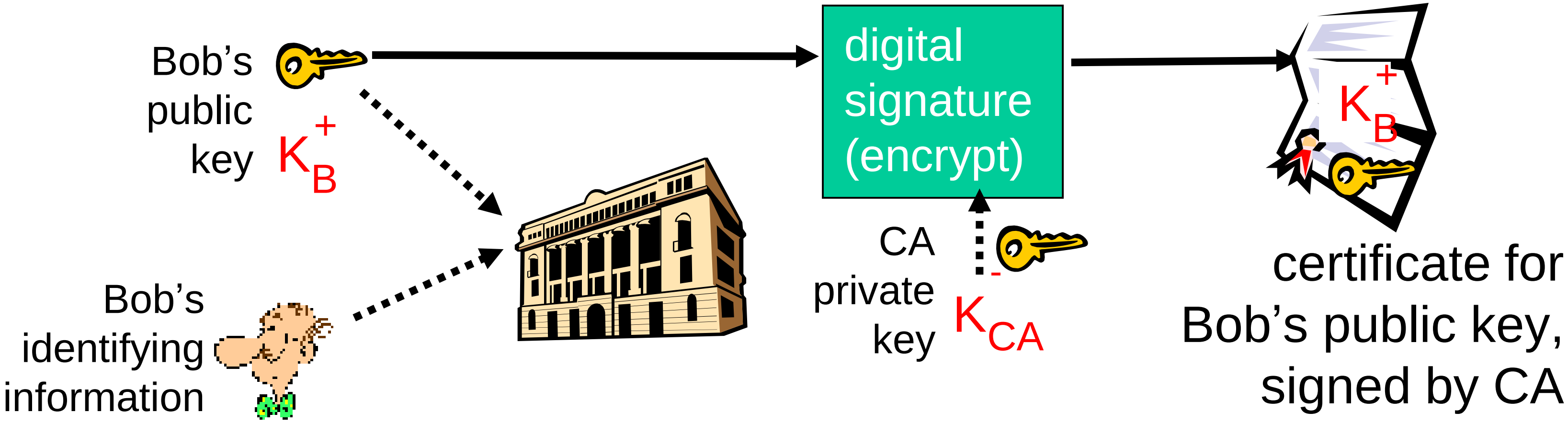
Only Bob can read this message and he knows that it is from Alice

Certificate Authorities

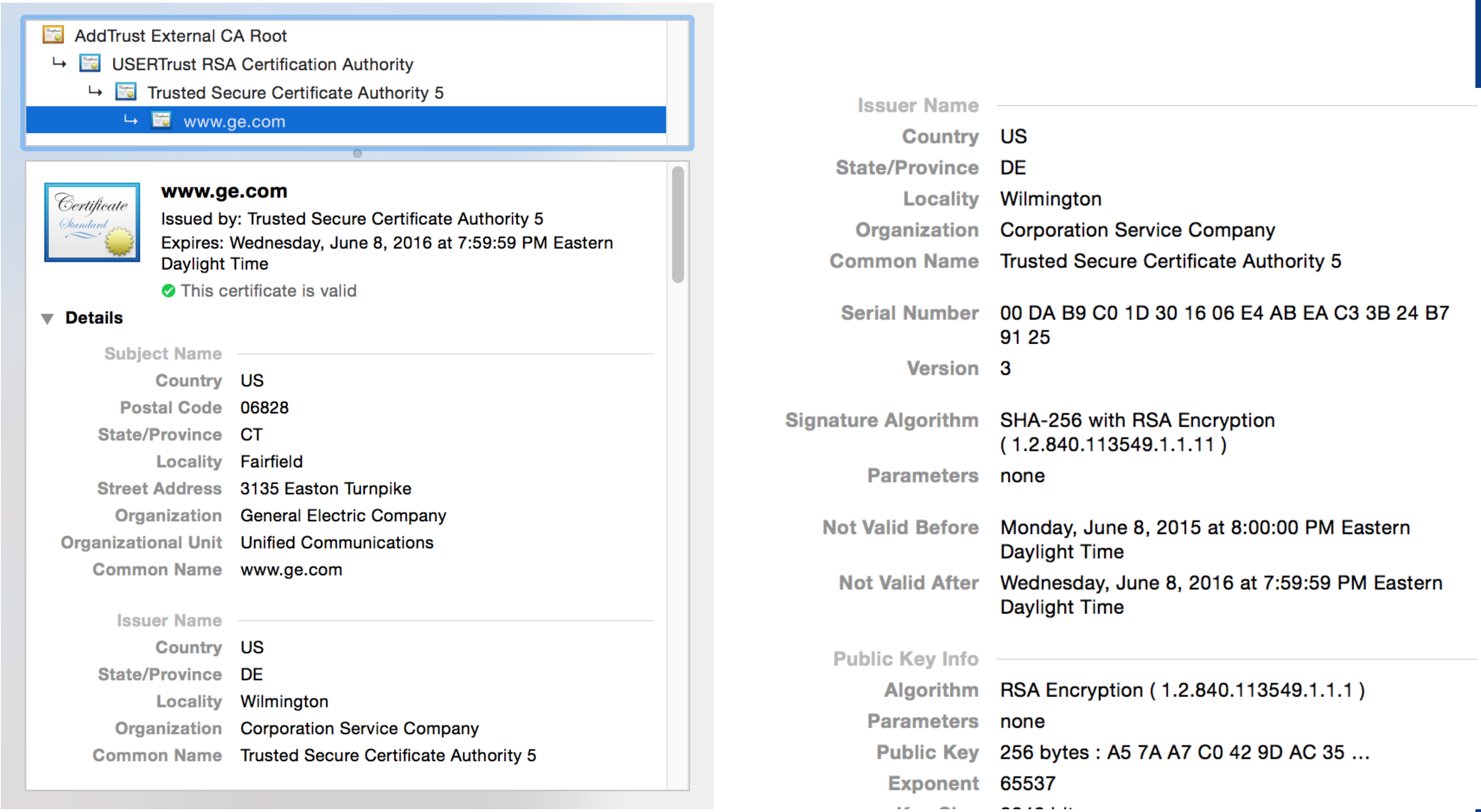
Certificate authority (CA): binds public key to particular entity, E.

E (person, router) registers its public key with CA.

- E provides “proof of identity” to CA.
- CA creates certificate binding E to its public key.
- certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”


Bob’s public key
K_B^+
digital signature (encrypt)
K_B^+
Bob’s identifying information
CA private key
K_{CA}^-
certificate for Bob’s public key, signed by CA

Example Certificate Contents



AddTrust External CA Root
↳ USERTrust RSA Certification Authority
↳ Trusted Secure Certificate Authority 5
↳ www.ge.com

www.ge.com
Issued by: Trusted Secure Certificate Authority 5
Expires: Wednesday, June 8, 2016 at 7:59:59 PM Eastern Daylight Time
✓ This certificate is valid

▼ **Details**

Subject Name
Country US
Postal Code 06828
State/Province CT
Locality Fairfield
Street Address 3135 Easton Turnpike
Organization General Electric Company
Organizational Unit Unified Communications
Common Name www.ge.com

Issuer Name
Country US
State/Province DE
Locality Wilmington
Organization Corporation Service Company
Common Name Trusted Secure Certificate Authority 5

Issuer Name
Country US
State/Province DE
Locality Wilmington
Organization Corporation Service Company
Common Name Trusted Secure Certificate Authority 5

Serial Number 00 DA B9 C0 1D 30 16 06 E4 AB EA C3 3B 24 B7 91 25
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

Not Valid Before Monday, June 8, 2015 at 8:00:00 PM Eastern Daylight Time
Not Valid After Wednesday, June 8, 2016 at 7:59:59 PM Eastern Daylight Time

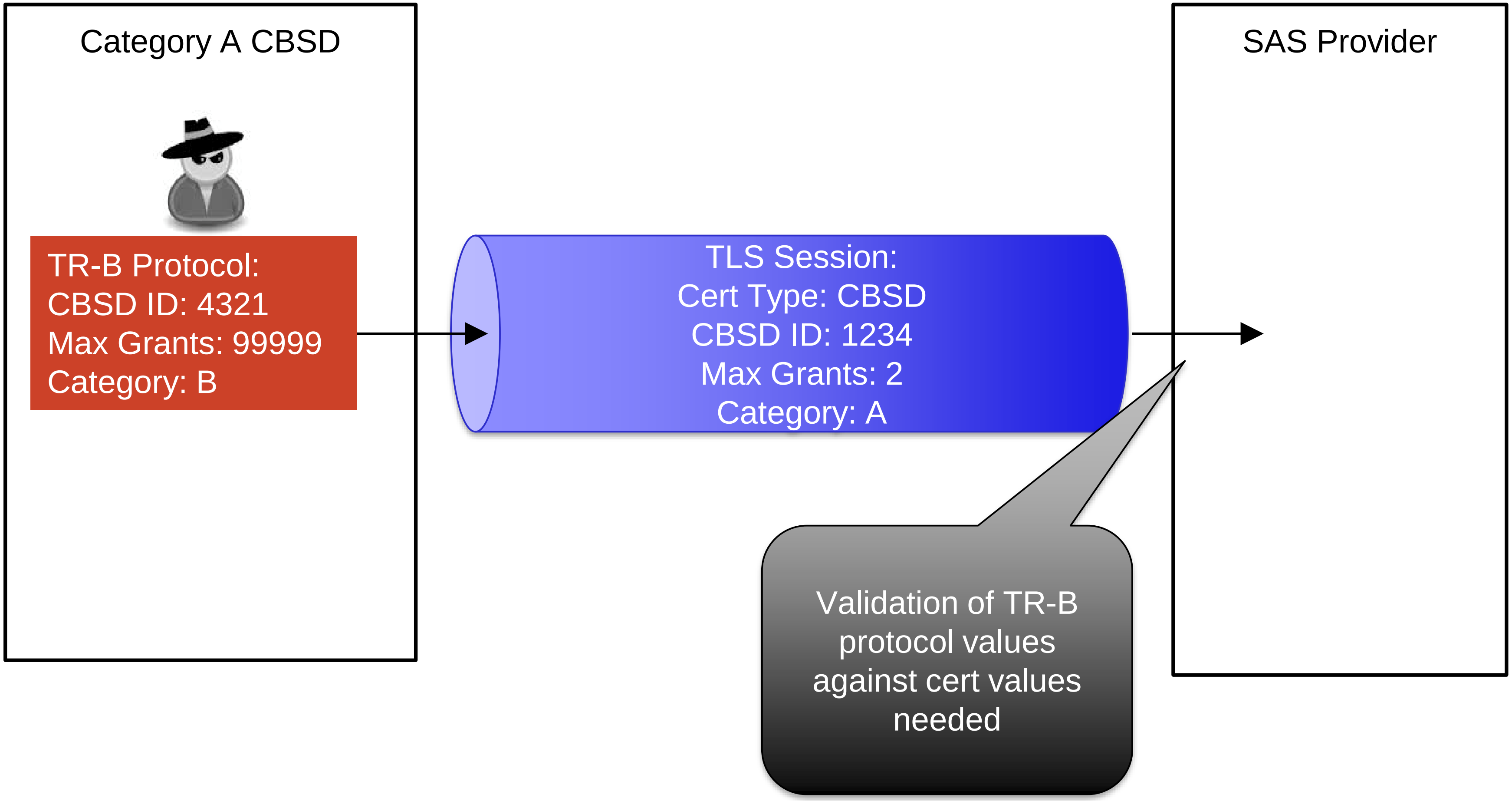
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 256 bytes : A5 7A A7 C0 42 9D AC 35 ...
Exponent 65537

CBRS Roles, Assets, and Trust Boundaries

Trust Boundary		Assets	Authentication Method
Source Entity	Target Entity		
Anonymous Internet Users	SAS	▪ SAS service availability ▪ SAS client credentials	None
CBSD Operators, Domain Proxy Operators, PAL Holders, Professional Installers	SAS	▪ Individual or Org to SAS Registration profiles, Authentication credentials ▪ Individual or Org service usage activity metadata	Proprietary – Per SAS Operator
CBSD, Domain Proxy	SAS	▪ CBSD/Domain Proxy to SAS Credentials, registration and other device metadata ▪ Spectrum grant and revocation data ▪ SAS Service availability	Standardized PKI
SAS	SAS	▪ SAS to SAS registration profiles, authentication credentials, and communication metadata ▪ SAS to SAS Communication data (including spectrum grants/revocations, obfuscated DoD spectrum usage metadata)	Standardized PKI for all SAS
ESC	SAS	▪ ESC to SAS Authentication credentials and communication metadata ▪ Obfuscated DoD channel usage metadata (Note: Specific DoD operational activity location data shall not be shared outside of ESC)	Proprietary – Per SAS Operator

CAs also hold valuable assets (ability to issue trusted certificates). Threats against cert issuance & revocation must be tracked and mitigated

Example: Masquerade Attack 1



Category A CBSD

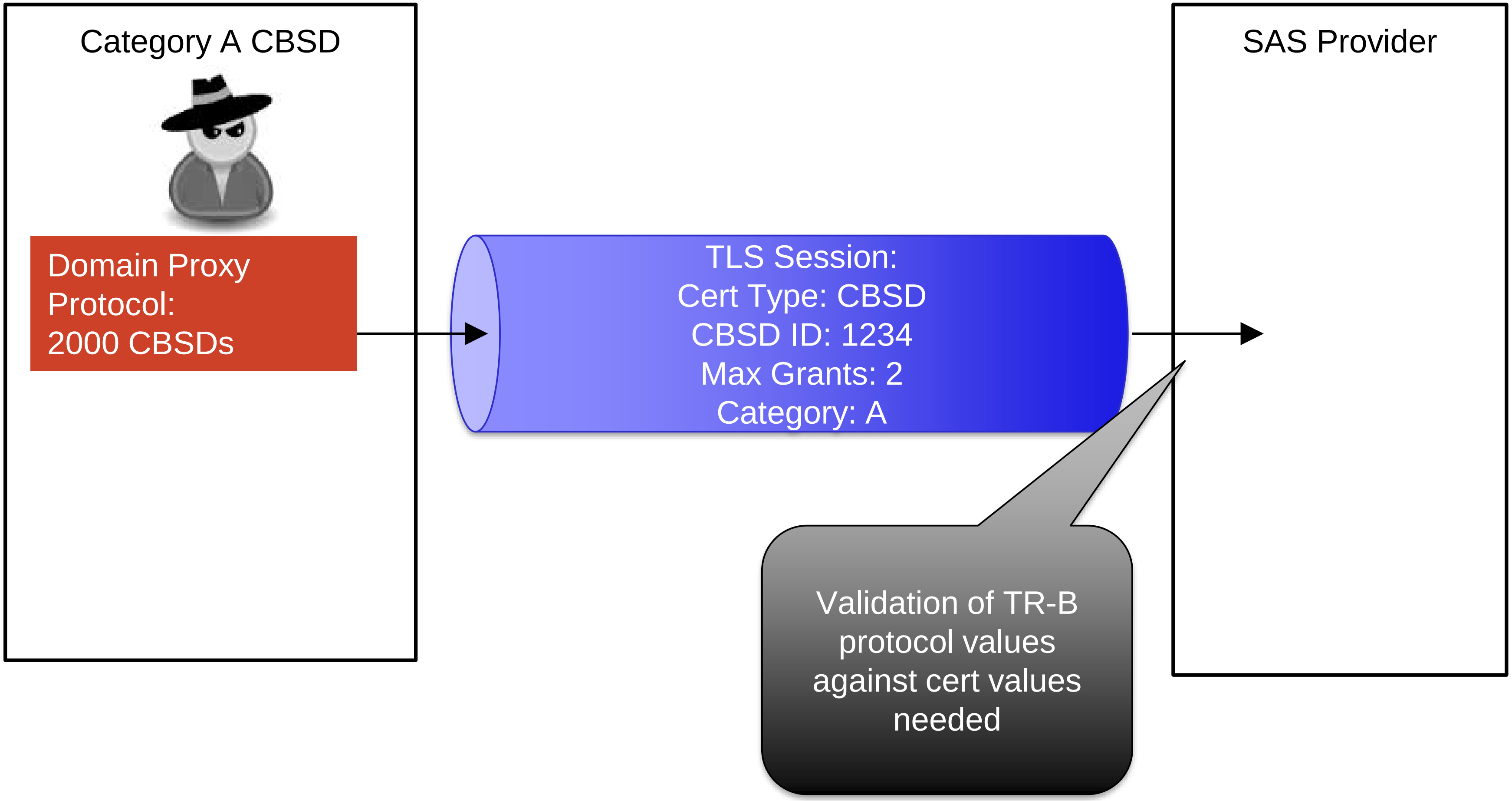
TR-B Protocol:
CBSD ID: 4321
Max Grants: 99999
Category: B

TLS Session:
Cert Type: CBSD
CBSD ID: 1234
Max Grants: 2
Category: A

SAS Provider

Validation of TR-B protocol values against cert values needed

Example: Masquerade Attack 2



Category A CBSD

Domain Proxy Protocol:
2000 CBSDs

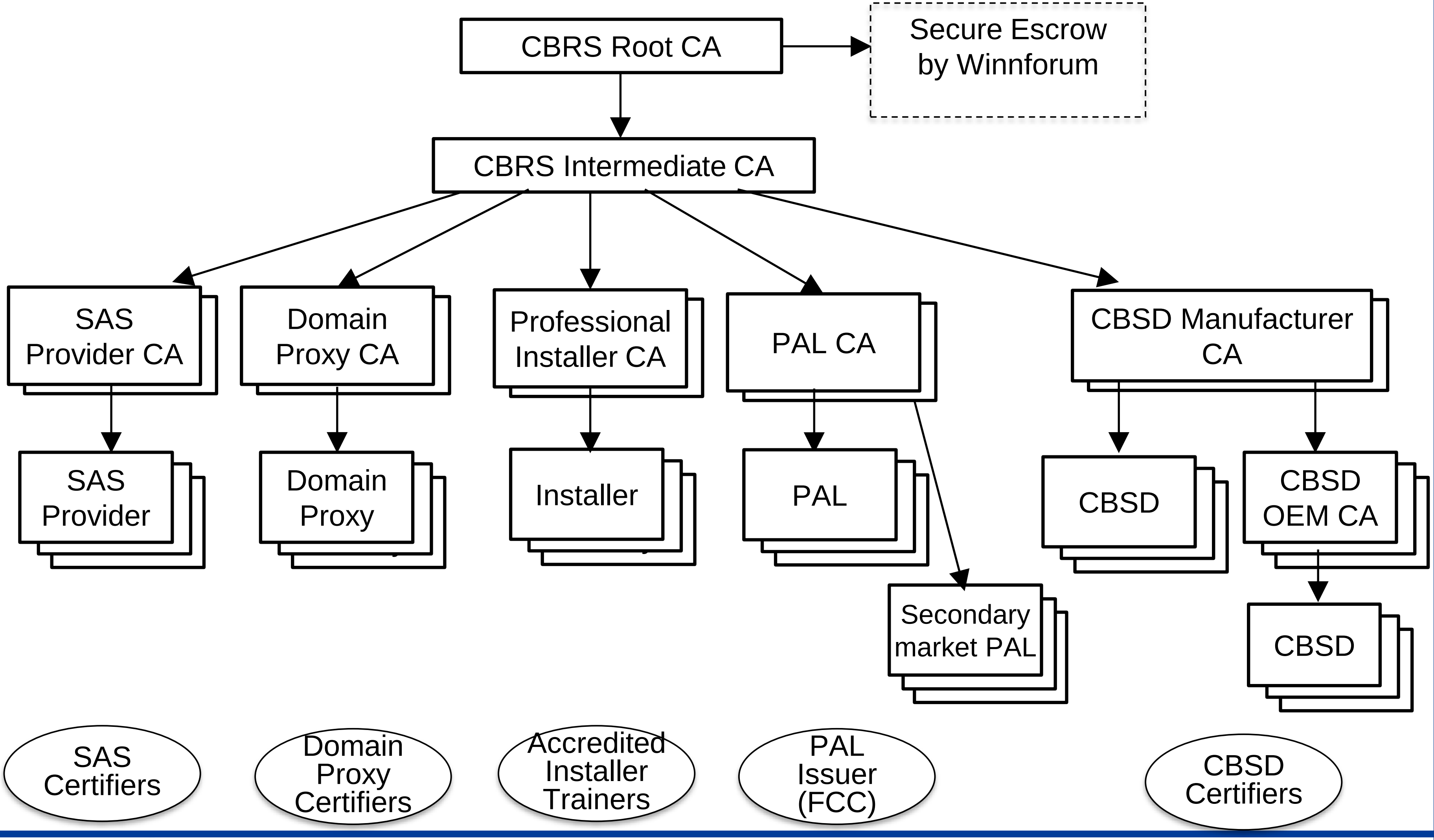
TLS Session:
Cert Type: CBSD
CBSD ID: 1234
Max Grants: 2
Category: A

SAS Provider

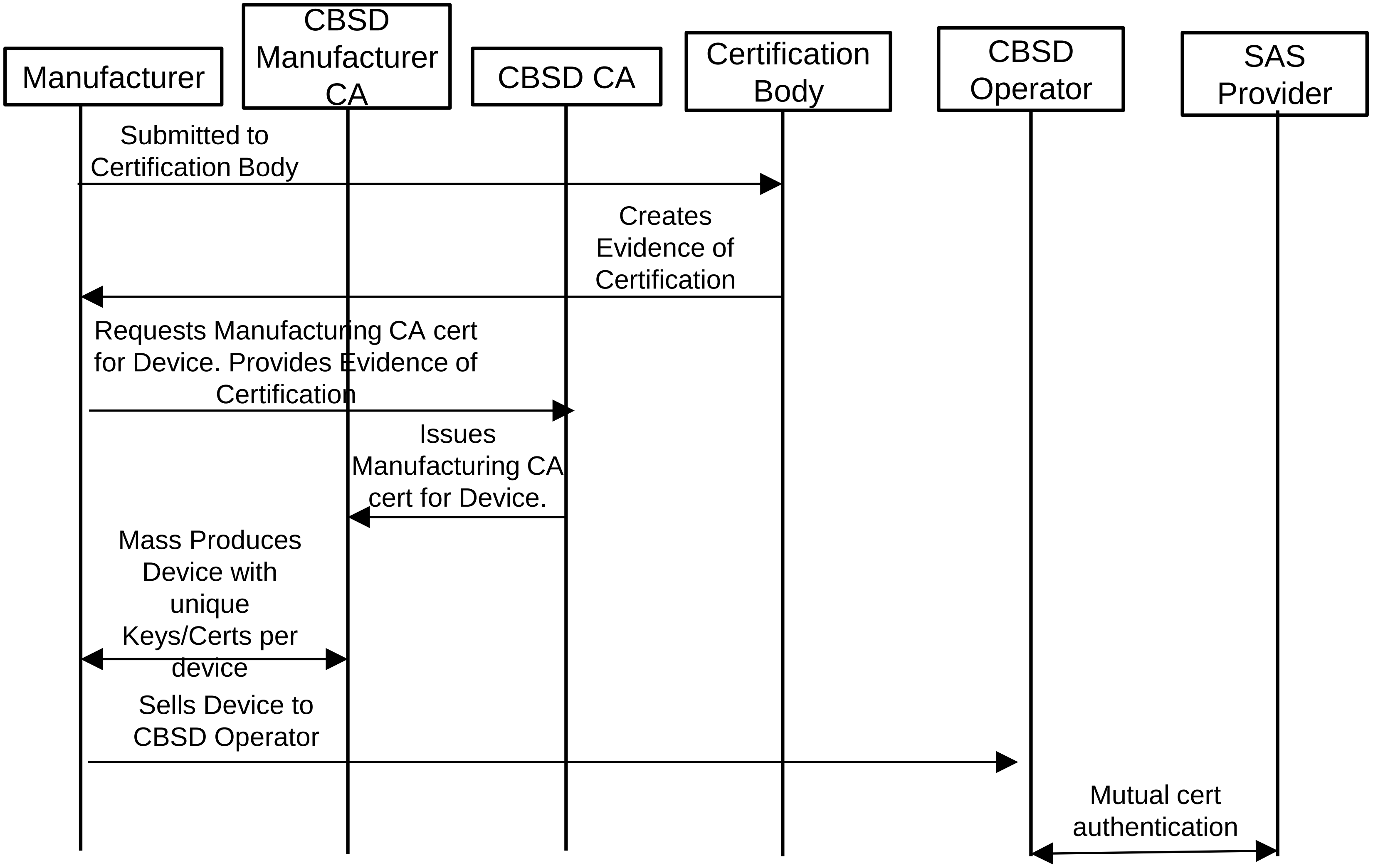
Validation of TR-B protocol values against cert values needed

CBRS PKI Hierarchy and Lifecycle

CBRS Certificate Trust Chains



CBSD Certificate Lifecycle



Manufacturer

CBSD Manufacturer CA

CBSD CA

Certification Body

CBSD Operator

SAS Provider

Submitted to Certification Body

Creates Evidence of Certification

Requests Manufacturing CA cert for Device. Provides Evidence of Certification

Issues Manufacturing CA cert for Device.

Mass Produces Device with unique Keys/Certs per device

Sells Device to CBSD Operator

Mutual cert authentication

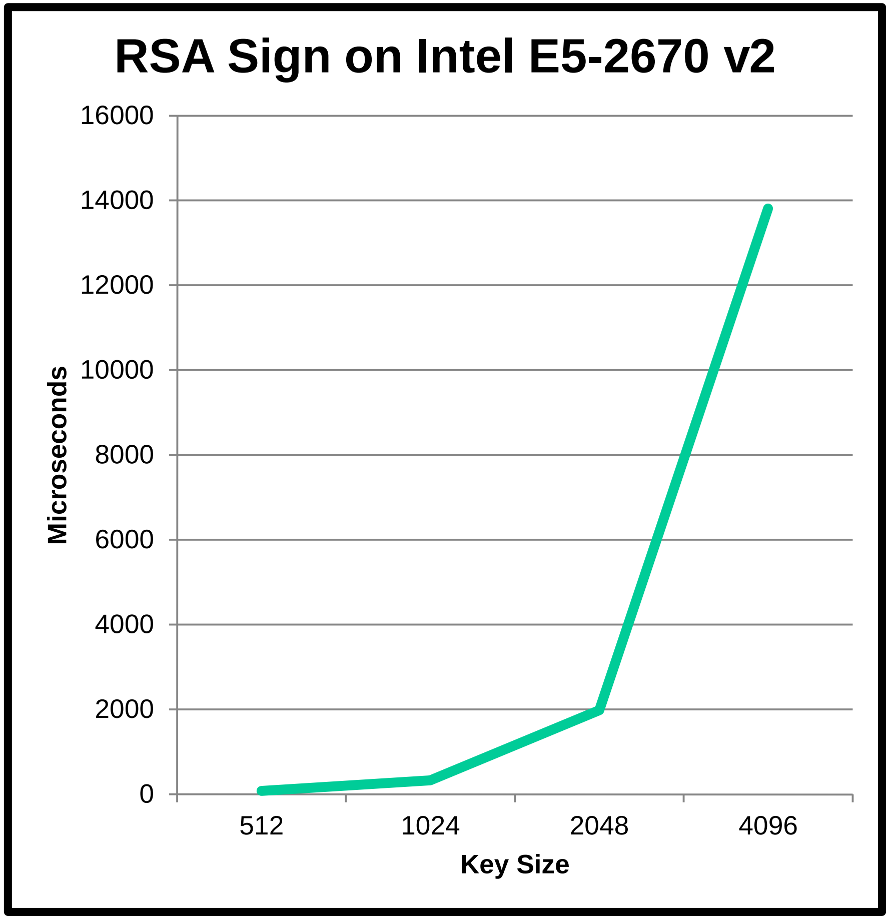
Key Lengths and Useful Crypto Life

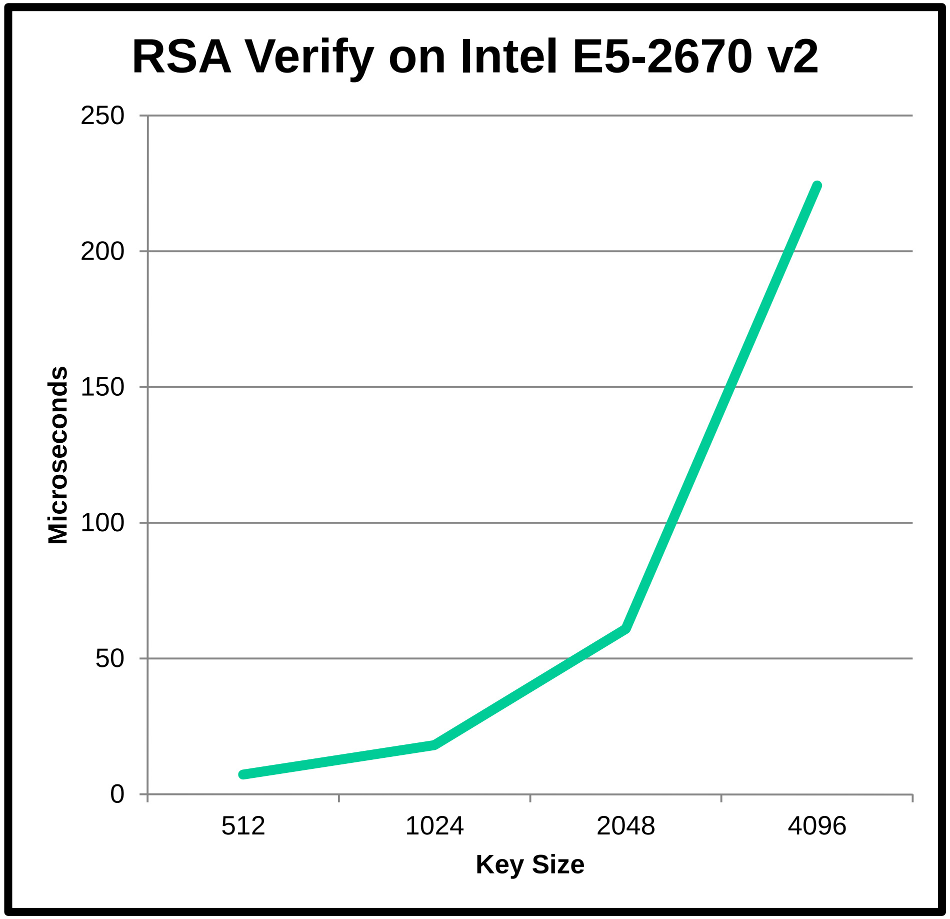
RSA Key Length	ECC Key Length	End of Useful Crypto Life
1024	160	2011
2048	224	2030
3072	256	~2042
4096	384	~2050

Exposure vs Rotation Periods

Role	Public Exposure	Cert Rotation Complexity	Validity Period	Private Key Material Protection Method
SAS Provider	High	Low (in cloud)	15 months	IT/Cloud services best practices
Domain Proxy	Medium/ Low	Medium Low (On prem or in cloud	15 months	IT/Cloud services best practices
Professional Installer	Low	Medium (human involvement)	27 months	Part of training program
PAL	Low	Medium	PAL Grant period	IT/Cloud services best practices
CBSD	Low	High	10 years	Under discussion: Hardware protection of private keys & firmware

Trade-off: CPU vs. Key Length





Role: CBRS Root

Holder	A single commercial CA contracted/commissioned by the Winnforum to generate and maintain the CBRS Root keys.
Purpose	Serve as a permanent root of trust for the CBRS ecosystem.
Usage	Only used to sign CBRS Intermediate CA certificates. (Very Rare)
Issuing CA	No upstream CA used. Generated as fresh keys by a CA, with backups in escrow.
Verification Requirements for Issuance	Contract with Winnforum (Winnforum pays the CA) Webtrust v2 certification
X509v3 certificate extensions	Role: CBRS Root
Level of Automation possible during issuance	None (Requires intentionally slow/difficult/expensive key generation ceremony)
Communication method for Revocation	Email/News (Automatic revocation not possible because this cert is self signed)
Quantity of certificates	2xRSA key pairs (4096 bits), 2xECC key pairs (521 bits) with copies in escrow Initially use single RSA key pair operationally
Validity Period	40 years

Role: CBRS Intermediate CA

Holder	One commercial CAs wishing to provide CA services to the CBRS ecosystem. In the future, this may expand to multiple CAs as authorized by Winnforum.
Purpose	Serve as an online Intermediate CA for the full CBRS ecosystem.
Usage	Used to sign Role CA certificates used at the top of each certificate role chain
Issuing CA	Root CA
Verification Requirements for Issuance	Contract with Winnforum (CA pays Winnforum nominal fee for processing contract) Webtrust v2 certification
X509v3 certificate extensions	Role: CBRS Intermediate CA Operating Authority: Winnforum Contract ID?
Level of Automation possible during issuance	None (Requires intentionally slow/difficult/expensive key signing ceremony)
Communication method for Revocation	CRL
Quantity of certificates	One Initially (4096bit RSA)
Validity Period	40 years

Role: Role CA (SAS Provider CA, Domain Proxy CA, Professional Installer CA, PAL CA, or CBSD Manufacturer CA)

Holder	A few (small number) of commercial CAs wishing to provide CA services to one or more of the CBRS Entity Roles (CBRS SAS providers, DP Operators, Professional Installers, PAL Holders, and CBSD Manufacturers respectively)
Purpose	Anchor trust for each role
Usage	Used to sign certificates within the respective certificate role chains
Issuing CA	CBRS Intermediate CA
Verification Requirements for Issuance	Contract with Winnforum (CA pays Winnforum nominal fee for processing contract) Webtrust v2 certification
X509v3 certificate extensions	Role: SAS Provider CA, DP CA, Professional Installer CA, PAL CA, and CBSD Manufacturer CA Respectively Operating Authority: Winnforum Contract ID?
Level of Automation possible during issuance	None (Requires intentionally slow/difficult/expensive key signing ceremony)
Communication method for Revocation	CRL
Quantity of certificates	Small number, each being (4096bit RSA)
Validity Period	CBSD CA: 20 years, all others: 10 years.

Role: SAS Provider

Holder	Any entity operating a WF/FCC certified SAS
Purpose	Authentication to CBSD, DP, and peer SAS “clients”.
Usage	Presented at TLS end points of SAS provider
Issuing CA	SAS CA
Verification Requirements for Issuance	Documentation showing SAS has passed Winnforum, FCC certifications
X509v3 certificate extensions	Role: SAS Provider Operating Authority: WF/FCC Certification IDs
Level of Automation possible during issuance	None (Extended/Manual validation)
Communication method for Revocation	CRL + OCSP
Quantity of certificates	Small number. Initially: 2048bit RSA
Validity Period	15 months (1 year + 90 day grace)

Role: Domain Proxy

Holder	Any entity operating WF/FCC certified Domain Proxy
Purpose	Authentication into SAS Providers
Usage	Presented on each connection into a SAS
Issuing CA	DP CA
Verification Requirements for Issuance	Documentation showing DP has passed Winnforum, FCC? certifications
X509v3 certificate extensions	Role: Domain Proxy Operating Authority: WF/FCC/DoD Certitication IDs?
Level of Automation possible during issuance	None (Extended/Manual validation)
Communication method for Revocation	CRL+OCSP, or proprietary (as negotiated with SAS Operator)
Quantity of certificates	100-1,000. Initially: 2048bit RSA
Validity Period	15 months (1 year + 90 day grace)

Role: Professional Installer

Holder	Any Professional Installer meeting Winnforum training requirements
Purpose	Authenticate Class-B CBSD installation data provided by Professional Installers
Usage	Used by professional installers to Digitally sign installation data. This data, with signatures may be entered into CBSDs, DPs, or SAS directly? Includes: Lat, Long, Height, Height-type, Horizontal Accuracy, Vertical Accuracy, Indoor Deployment, Antennae Model
Issuing CA	PI CA with issuance requested by an accredited PI training program
Verification Requirements for Issuance	Evidence of successful completion of PI training program (supplied by Accredited PI training program).
X509v3 certificate extensions	Role: Professional Installer Operating Authority: PI training program ID + PI training program certificate Serial number?
Level of Automation possible during issuance	Manual verification of training program accreditations to form relationship with PI CA. Fully Automated once PI Training program forms relationship with PI CA. PI CA exposes web interface to PI training program to request and issue certificates.
Communication method for Revocation	CRL+OCSP
Quantity of certificates	1,000-10,000? 4096bit RSA
Validity Period	27 months

Role: Prioritized Access License (PAL) and Secondary PALs

Holder	Any PAL Holder
Purpose	Authorize prioritization of bandwidth allocation within a given census tract.
Usage	Used by CBSDs or DPs to request spectrum. PAL certs may be used to sign CBSD Certs, or DP Certs, or used to interact with SAS directly?
Issuing CA	PAL CA
Verification Requirements for Issuance	Primary: Evidence of FCC PAL grant ownership Secondary: PAL Cert ownership In the case of Secondary PALs: PAL Holders Trade in their primary PAL Certs to the CA (which are revoked), to be subdivided into multiple time/geo restricted certs.
X509v3 certificate extensions	Role: PAL Operating Authority: FCC PAL ID Census Tract IDs Bandwidth
Level of Automation possible during issuance	Primary: Manual Verification required? (any way to automate verification of PAL ownership?) Secondary: Exchange Primary PAL certificate with CA for Secondary Certs
Communication method for Revocation	CRL+OCSP or proprietary protocol/agreement between PAL CA and SA provider
Quantity of certificates	A few hundred K to a few Million. 4096bit RSA
Validity Period	Life of FCC PAL grant

Role: CBSD

Holder	Any entity operating WF/FCC certified CBSD
Purpose	Authentication into SAS Providers Authentication of manufacture time CBSD characteristics
Usage	Presented on each connection into a SAS
Issuing CA	CBSD CA or CBSD OEM CA
Verification Requirements for Issuance	Documentation showing CBSD has passed Winnforum, FCC Certifications FCC ID Device Serial Number
X509v3 certificate extensions	Role: CBSD FCC Operating Authority: FCC ID Serial Number Maximum Grants
Level of Automation possible during issuance	CBSD CA or CBSD OEM CA provide interface (GUI/API) to CBSD Manufacturer to request certificates
Communication method for Revocation	CRL + OCSP, or proprietary (as negotiated with SAS Operator)
Quantity of certificates	Millions. 4096bit RSA
Validity Period	10 years? (See “Trade-offs” Slide)

Role: CBSD OEM CA

Holder	Any CBSD Manufacturer operating their own CA (wishing to issue their own certificates)
Purpose	Signing 1 level down of CBSD certificates
Usage	Issue CBSD certificates.
Issuing CA	CBSD CA
Verification Requirements for Issuance	Documentation showing CBSD has passed Winnforum/FCC Certifications FCC ID Webtrust v2 certification
X509v3 certificate extensions	Role: CBSD FCC Operating Authority: FCC ID Maximum Grants
Level of Automation possible during issuance	Manual (Extended validation)
Communication method for Revocation	CRL+OCSP, or proprietary (as negotiated with SAS Operator)
Quantity of certificates	Hundreds. 4096bit RSA
Validity Period	10 years? (See “Trade-offs” Slide)

Webtrust Summary (Required for all CAs)

From NAESB Presentation

CA ENVIRONMENTAL CONTROLS	CA KEY MANAGEMENT	CERTIFICATE LIFE CYCLE MANAGEMENT
• CP/CPS Management • Security Management • Asset Classification and Management • Personnel Security • Physical and Environmental Security • Operations Management • System Access Management • Systems Development and Maintenance • Business Continuity Management • Monitoring and Compliance • Event Journaling	• CA Key Generation • CA Key Storage Backup and Recovery • CA Key Escrow (optional) • CA Key Usage • CA Key Archival • CA Key Destruction • CA Cryptographic Device Life Cycle Management • CA-Provided Subscriber Key Management Services (optional)	• Subscriber Registration • Certificate Rekey/ Renewal Certificate Issuance • Certificate Distribution • Certificate Revocation • Certificate Suspension (optional) • Certificate Status Information Processing • Integrated Circuit Card Life Cycle Management (optional)

Next Steps

- Discuss CBSD manufacturer concerns regarding single/external root of trust
- Common agreement on verification requirements for cert issuance (for each type)
- Need clear policy for PAL cert issuance, usage, and lifecycles
- Need clear policy for PI cert issuance, usage and lifecycles
- Formal Winnforum contract needed to govern behavior of entities wishing to perform CA responsibilities in the CBRS ecosystem.

Questions/Discussion