Security, Certificates, and the System Administrator

ConvergeOne AVAYA ENGAGE®

Chris Clauss

Manager, Avaya UC Engineering

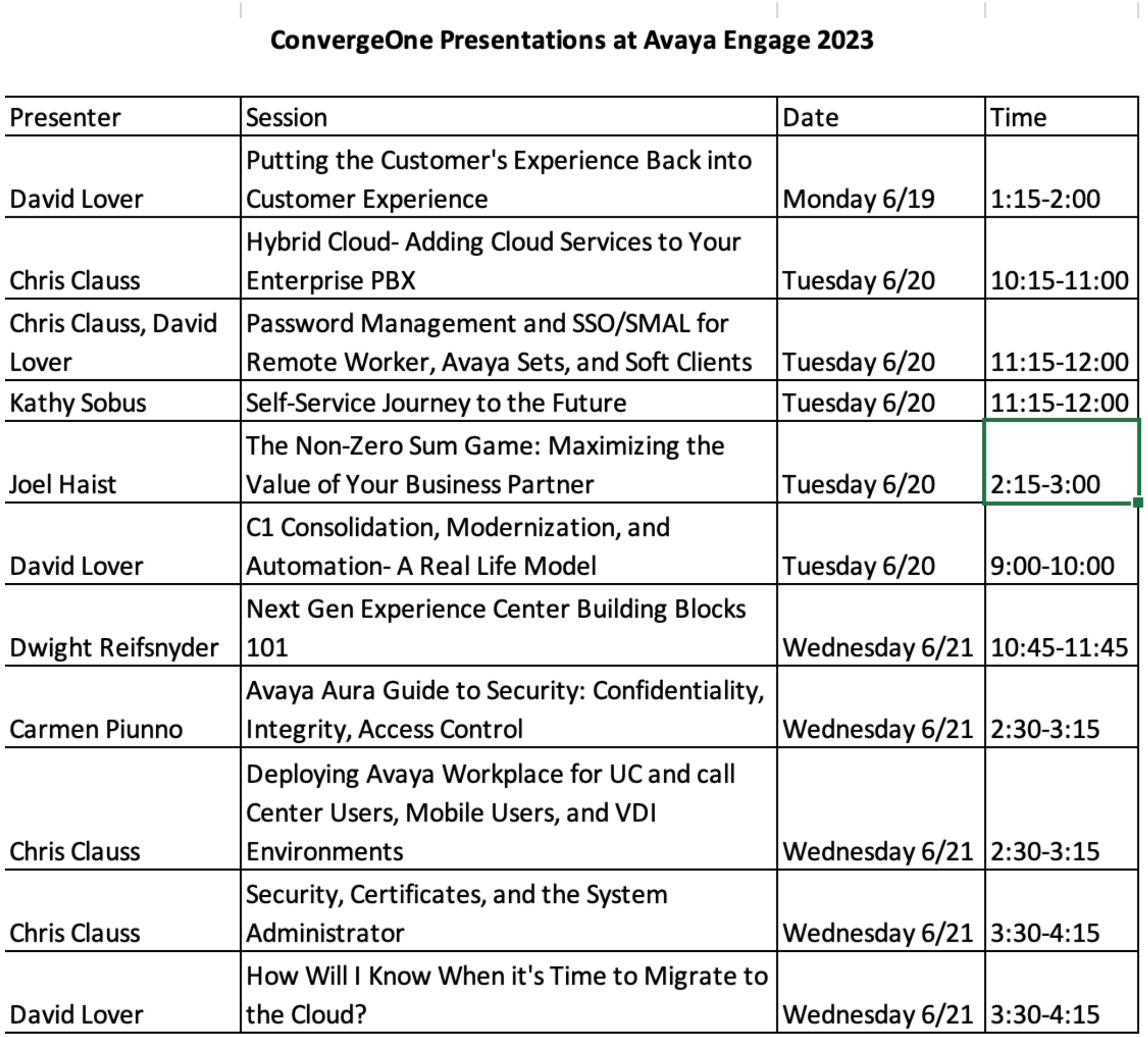
Collaboration

ConvergeOne

Feel The Impact

ConvergeOne

Visit our Other Sessions!



ConvergeOne Presentations at Avaya Engage 2023

Presenter	Session	Date	Time
David Lover	Putting the Customer's Experience Back into Customer Experience	Monday 6/19	1:15-2:00
Chris Clauss	Hybrid Cloud- Adding Cloud Services to Your Enterprise PBX	Tuesday 6/20	10:15-11:00
Chris Clauss, David Lover	Password Management and SSO/SMAL for Remote Worker, Avaya Sets, and Soft Clients	Tuesday 6/20	11:15-12:00
Kathy Sobus	Self-Service Journey to the Future	Tuesday 6/20	11:15-12:00
Joel Haist	The Non-Zero Sum Game: Maximizing the Value of Your Business Partner	Tuesday 6/20	2:15-3:00
David Lover	C1 Consolidation, Modernization, and Automation- A Real Life Model	Tuesday 6/20	9:00-10:00
Dwight Reifsnyder	Next Gen Experience Center Building Blocks 101	Wednesday 6/21	10:45-11:45
Carmen Piunno	Avaya Aura Guide to Security: Confidentiality, Integrity, Access Control	Wednesday 6/21	2:30-3:15
Chris Clauss	Deploying Avaya Workplace for UC and call Center Users, Mobile Users, and VDI Environments	Wednesday 6/21	2:30-3:15
Chris Clauss	Security, Certificates, and the System Administrator	Wednesday 6/21	3:30-4:15
David Lover	How Will I Know When it's Time to Migrate to the Cloud?	Wednesday 6/21	3:30-4:15

What is or will be driving security in your organization?

- Devices
  - Remote Worker
  - Internet Connected Device
  - BYOD
  - Hosted Solutions
- Security Teams
  - Are they asking for audits?
  - Are they taking notice of U/C?
  - Is management worried (news)?
- What needs to be secured?
  - Voice conversations
  - The systems themselves

A brief introduction to security…

A security system must provide: (CIA+A)

- **Confidentiality**
- **Integrity**
- **Availability**
- **Authentication**

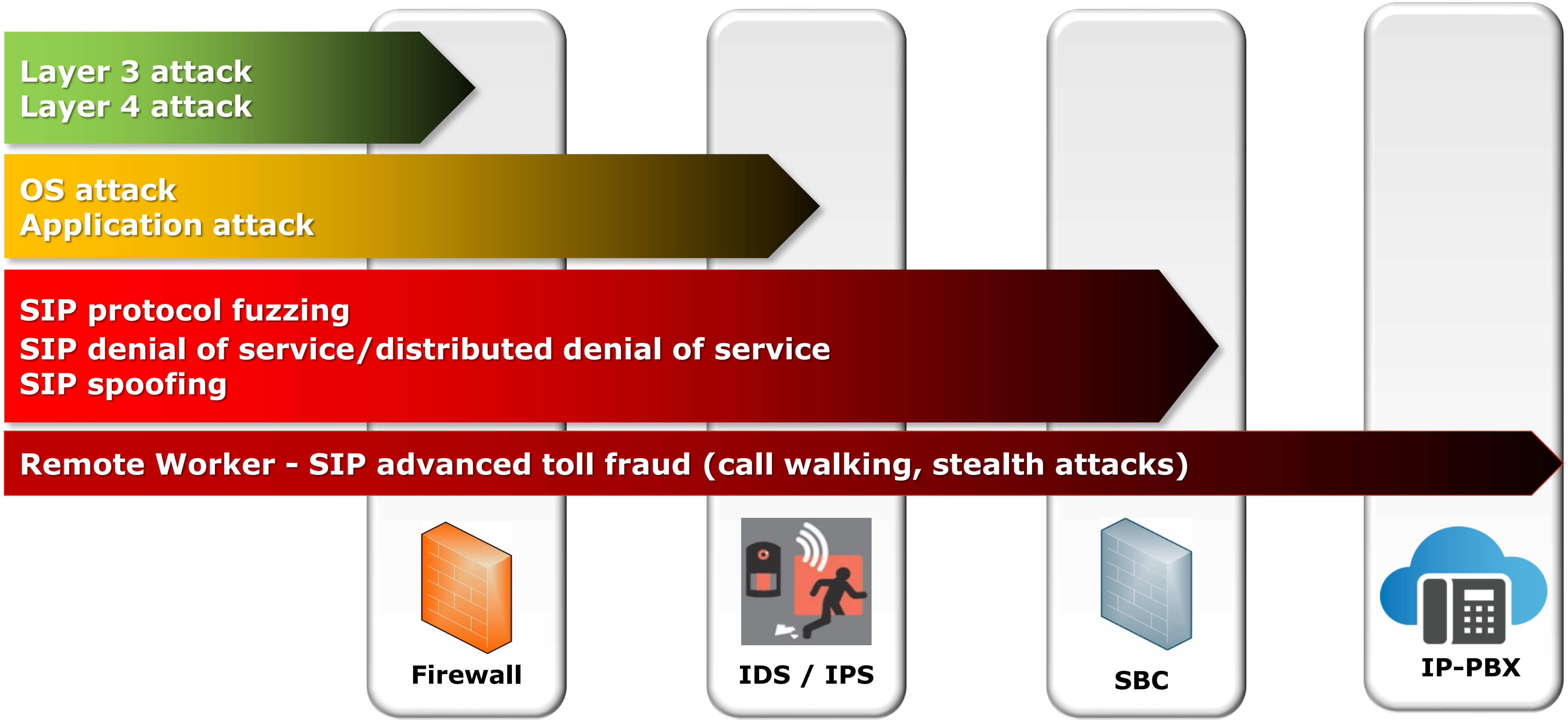
Security systems must make the cost of attacking an asset higher than the value of the asset being attacked.

- Failure to provide adequate security:
  - Exposure or loss of information
  - Loss of time, money, or capital resources.
  - Legal exposure (liability).
  - Loss of credibility, trust, or market share.

A brief introduction to security…

- Confidentiality
  - Ensuring no eavesdropping – keeping information private.
- Availability
  - Protecting from Denial-of-Service attacks, System Hacks
- Integrity
  - Ensure data cannot be manipulated.
- Authentication
  - Insure the identity of people or applications.

U/C Security is Different from Data security



Layer 3 attack
Layer 4 attack

OS attack
Application attack

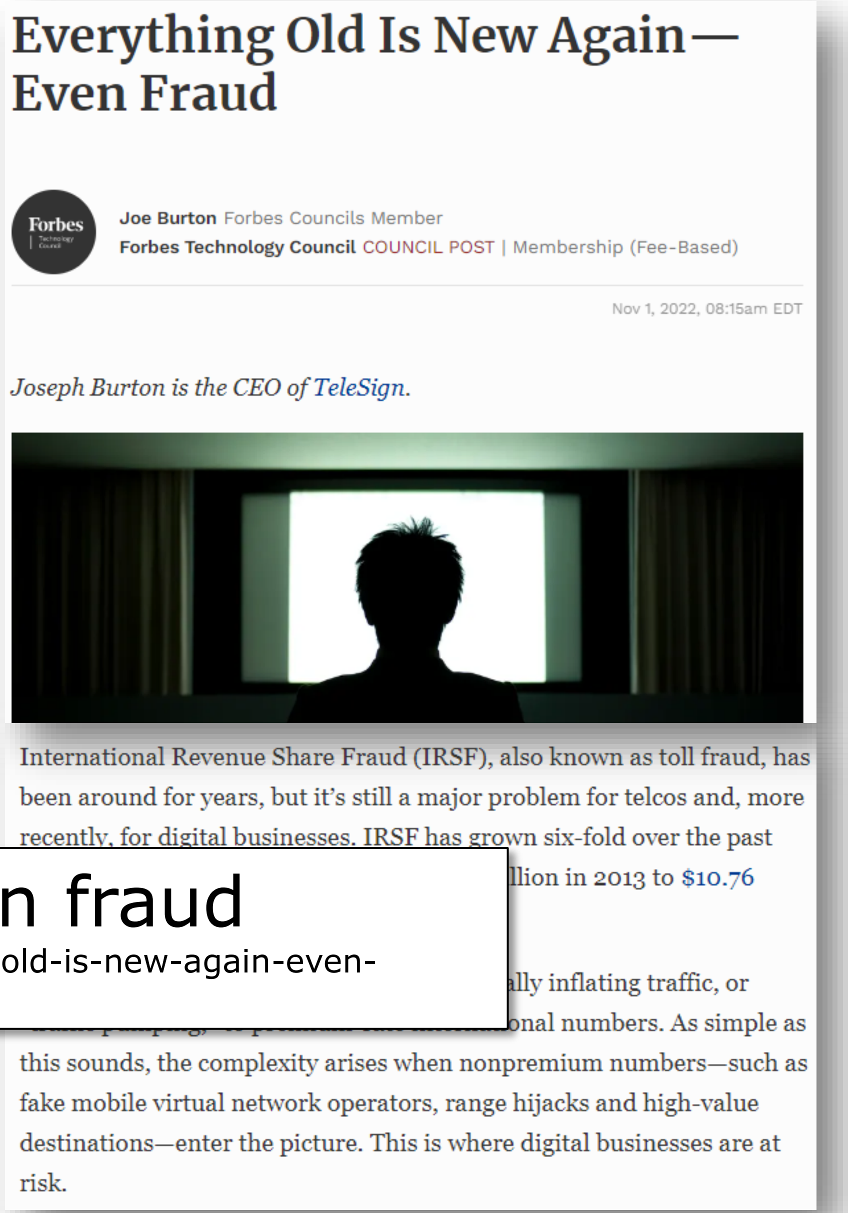
SIP protocol fuzzing
SIP denial of service/distributed denial of service
SIP spoofing

Remote Worker - SIP advanced toll fraud (call walking, stealth attacks)

VOIP Security requires deep understanding of the requirements of UC

Are the security threats for real?

"IRSF has grown six-fold over the past decade, with total losses leaping from $1.8 billion in 2013 to $10.76 billion today."



Everything Old Is New Again—Even Fraud

Forbes Technology Council

Joe Burton Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Nov 1, 2022, 08:15am EDT

Joseph Burton is the CEO of TeleSign.

International Revenue Share Fraud (IRSF), also known as toll fraud, has been around for years, but it's still a major problem for telcos and, more recently, for digital businesses. IRSF has grown six-fold over the past

llion in 2013 to $10.76

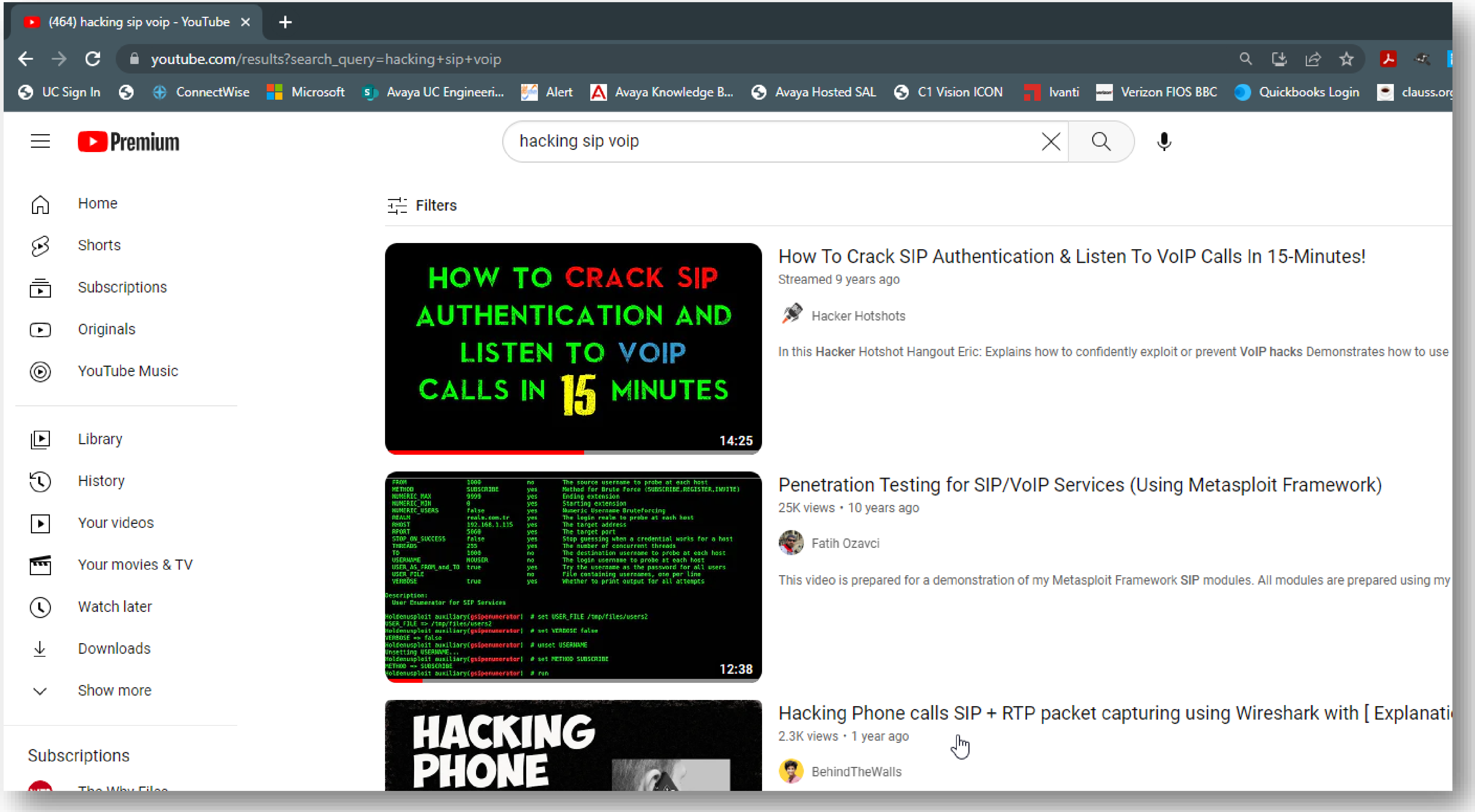
lly inflating traffic, or

onal numbers. As simple as this sounds, the complexity arises when nonpremium numbers—such as fake mobile virtual network operators, range hijacks and high-value destinations—enter the picture. This is where digital businesses are at risk.

Everything old is new again – even fraud

https://www.forbes.com/sites/forbestechcouncil/2022/11/01/everything-old-is-new-again-even-fraud/?sh=3a0272b2126d

Are the security threats for real?



How To Crack SIP Authentication & Listen To VoIP Calls In 15-Minutes!

Streamed 9 years ago

Hacker Hotshots

In this Hacker Hotshot Hangout Eric: Explains how to confidently exploit or prevent VoIP hacks Demonstrates how to use

```
 FROM              1000          no     The source username to probe at each host
 METHOD            SUBSCRIBE     yes    Method for Brute Force (SUBSCRIBE,REGISTER,INVITE)
 NUMERIC_MAX       9999          yes    Ending extension
 NUMERIC_MIN       0             yes    Starting extension
 NUMERIC_USERS     false         yes    Numeric Username Bruteforcing
 REALM             realm.com.tr  yes    The login realm to probe at each host
 RHOST             192.168.1.115 yes    The target address
 RPORT             5060          yes    The target port
 STOP_ON_SUCCESS   false         yes    Stop guessing when a credential works for a host
 THREADS           255           yes    The number of concurrent threads
 TO                1000          no     The destination username to probe at each host
 USERNAME          NOUSER        no     The login username to probe at each host
 USER_AS_FROM_and_TO true        yes    Try the username as the password for all users
 USER_FILE                       no     File containing usernames, one per line
 VERBOSE           true          yes    Whether to print output for all attempts

Description:
 User Enumerator for SIP Services

Holdenusploit auxiliary(gsipenumerator)  # set USER_FILE /tmp/files/users2
USER_FILE => /tmp/files/users2
Holdenusploit auxiliary(gsipenumerator)  # set VERBOSE false
VERBOSE => false
Holdenusploit auxiliary(gsipenumerator)  # unset USERNAME
Unsetting USERNAME...
Holdenusploit auxiliary(gsipenumerator)  # set METHOD SUBSCRIBE
METHOD => SUBSCRIBE
Holdenusploit auxiliary(gsipenumerator)  # run
```

Penetration Testing for SIP/VoIP Services (Using Metasploit Framework)

25K views • 10 years ago

Fatih Ozavci

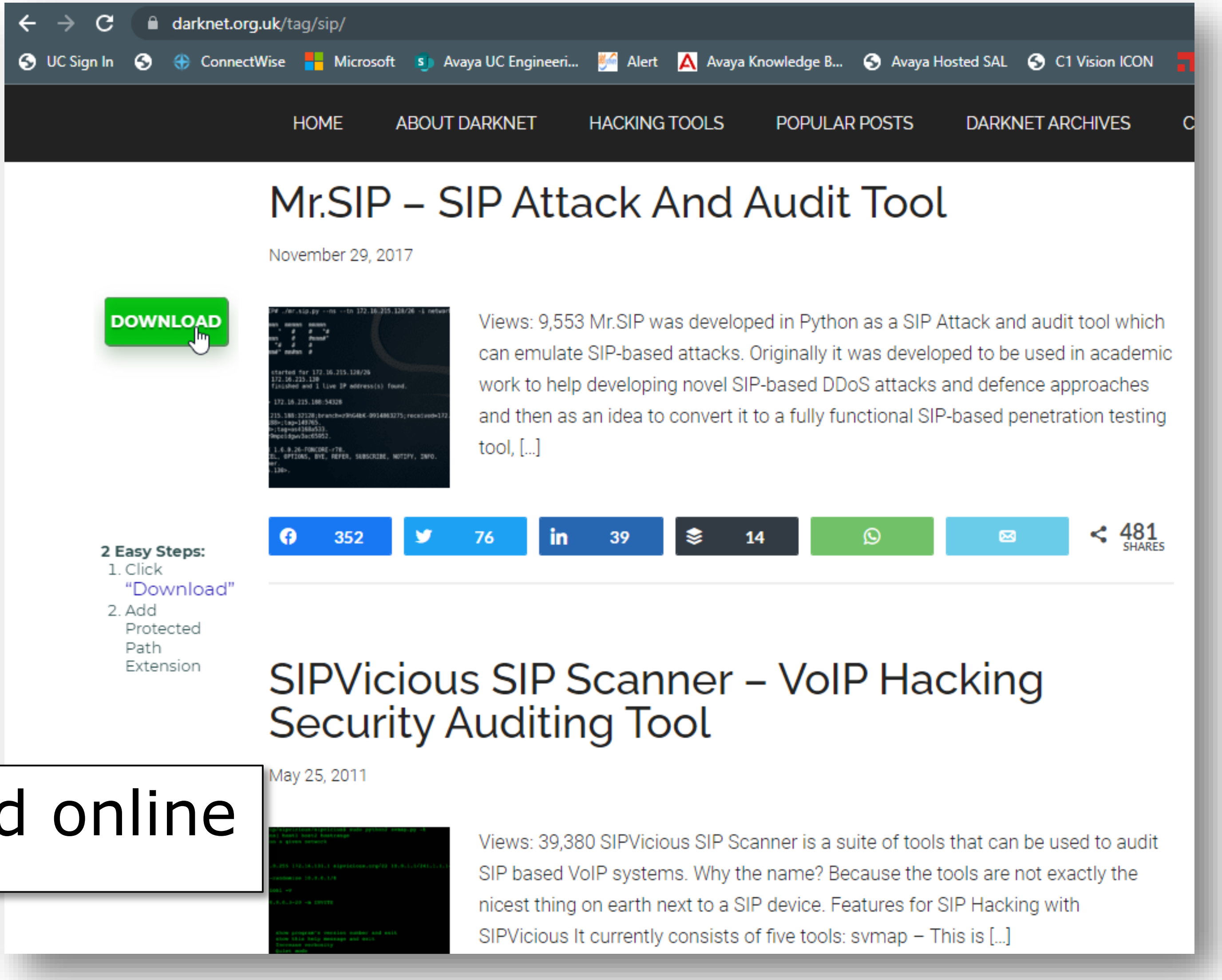
This video is prepared for a demonstration of my Metasploit Framework SIP modules. All modules are prepared using my

Hacking Phone calls SIP + RTP packet capturing using Wireshark with [Explanati

2.3K views • 1 year ago

BehindTheWalls

Are the security threats for real?



2 Easy Steps:

1. Click "Download"
2. Add Protected Path Extension

Mr.SIP – SIP Attack And Audit Tool

November 29, 2017

Views: 9,553 Mr.SIP was developed in Python as a SIP Attack and audit tool which can emulate SIP-based attacks. Originally it was developed to be used in academic work to help developing novel SIP-based DDoS attacks and defence approaches and then as an idea to convert it to a fully functional SIP-based penetration testing tool, [...]

SIPVicious SIP Scanner – VoIP Hacking Security Auditing Tool

May 25, 2011

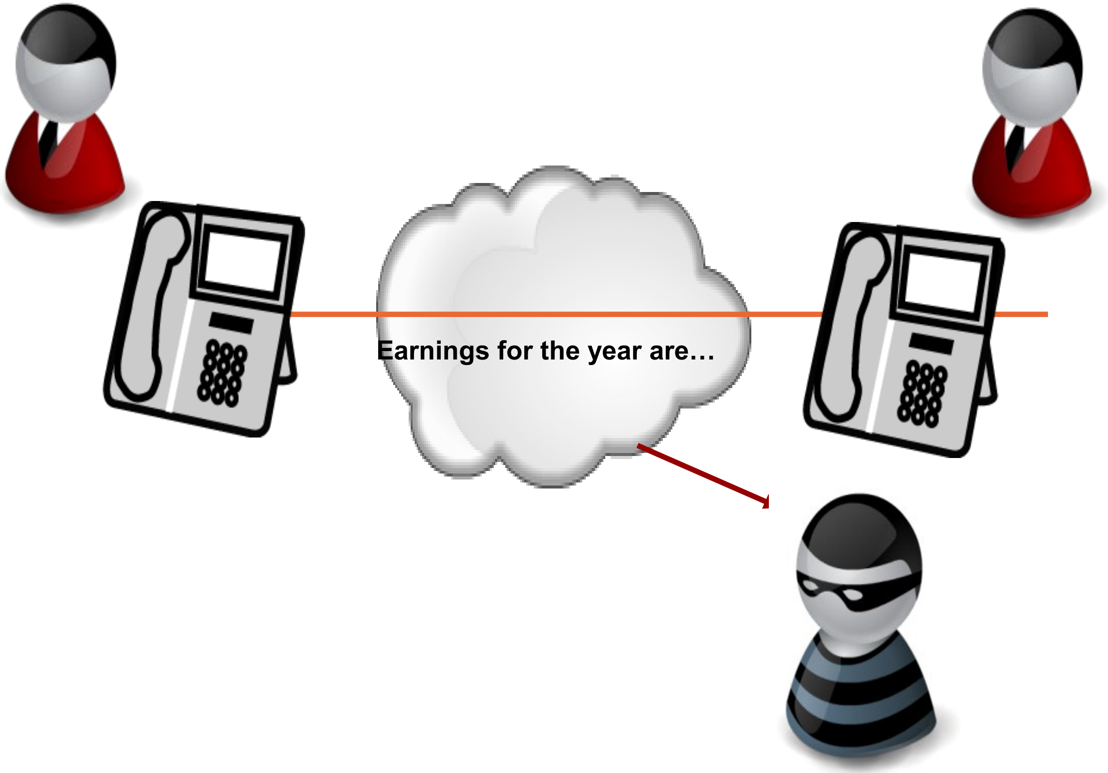
Views: 39,380 SIPVicious SIP Scanner is a suite of tools that can be used to audit SIP based VoIP systems. Why the name? Because the tools are not exactly the nicest thing on earth next to a SIP device. Features for SIP Hacking with SIPVicious It currently consists of five tools: svmap – This is [...]

Tools are easily found online

https://www.darknet.org.uk/tag/sip/

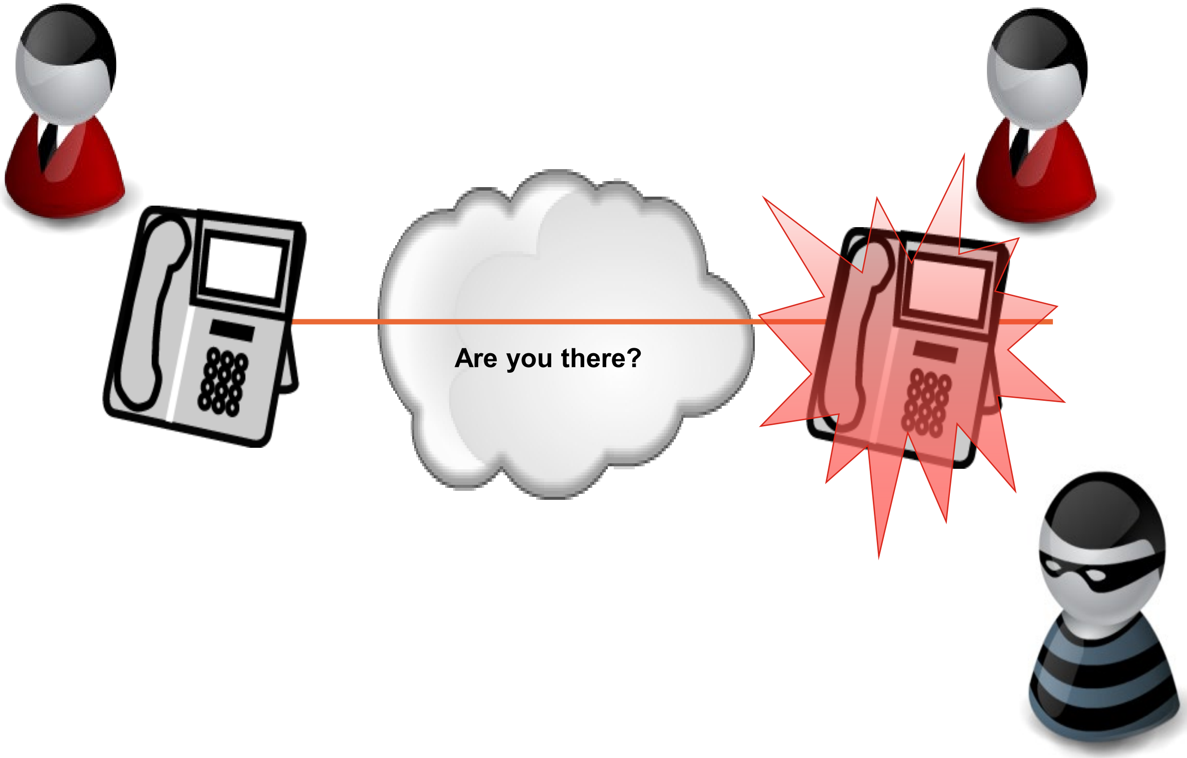
Confidentiality Attacks – is someone listening in?

- Eavesdropping signaling –
  Who calls whom and when?
- Eavesdropping media –
  Obtaining voice, fax, video, data.
- Remote software exploits –
  Theft of confidential data.



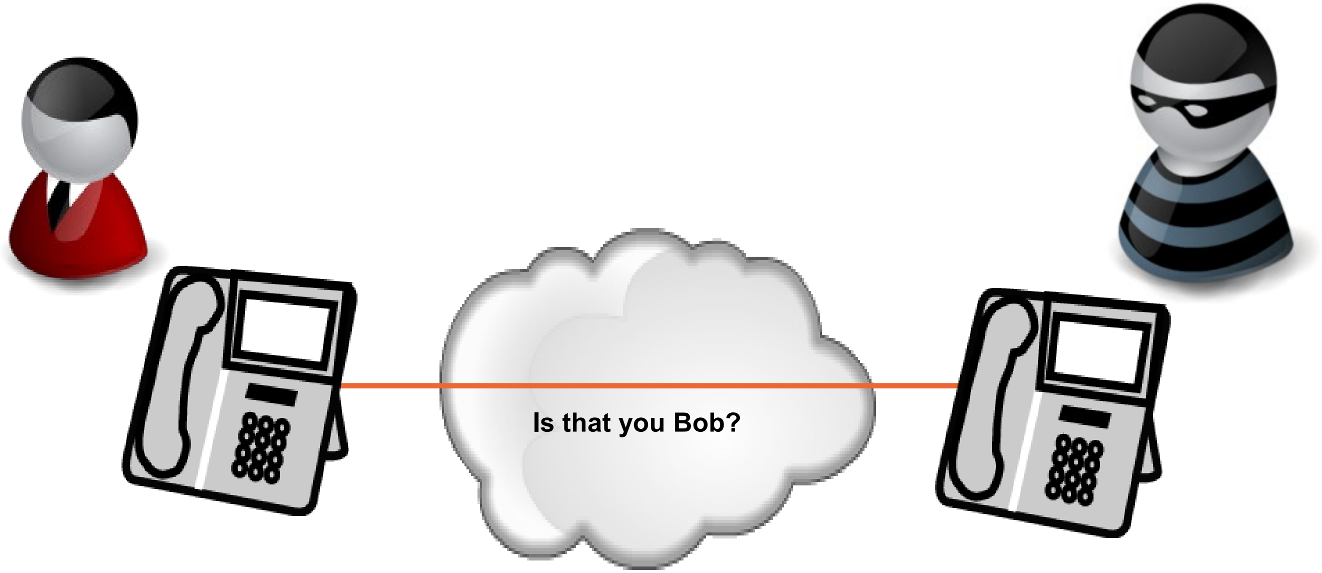
Availability Attacks – Denial of Service

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) floods – network layer, SIP layer.
- Fuzzing applications that send malformed SIP or RTP to test for security vulnerabilities or crash the voice system.
- Stealth DoS such as harassment (phone rings every 5 minutes)

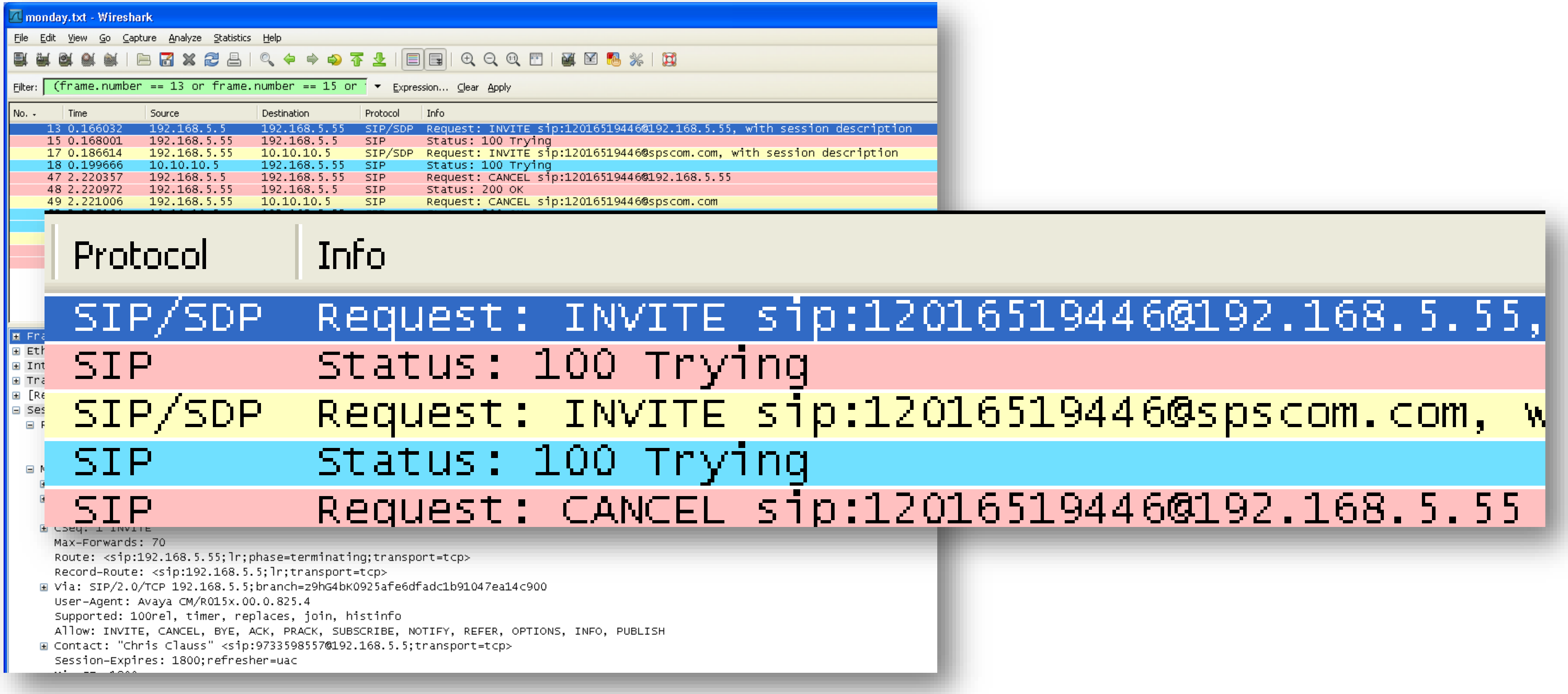


Security Attacks - Authentication (e.g. Toll Fraud)

- Unauthorized toll calls placed by internal or external users.
- Intercepting dial patterns to retrieve access codes.
- Using SIP methods to transfer sessions.



VOIP Trace – What’s the problem with this picture?


monday.txt - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
(frame.number == 13 or frame.number == 15 or
```

```
No.   Time      Source        Destination   Protocol  Info
   13 0.166032  192.168.5.5   192.168.5.55  SIP/SDP   Request: INVITE sip:12016519446@192.168.5.55, with session description
   15 0.168001  192.168.5.55  192.168.5.5   SIP       Status: 100 Trying
   17 0.186614  192.168.5.55  10.10.10.5    SIP/SDP   Request: INVITE sip:12016519446@spscom.com, with session description
   18 0.199666  10.10.10.5    192.168.5.55  SIP       Status: 100 Trying
   47 2.220357  192.168.5.5   192.168.5.55  SIP       Request: CANCEL sip:12016519446@192.168.5.55
   48 2.220972  192.168.5.55  192.168.5.5   SIP       Status: 200 OK
   49 2.221006  192.168.5.55  10.10.10.5    SIP       Request: CANCEL sip:12016519446@spscom.com
```

```
Protocol   Info
SIP/SDP    Request: INVITE sip:12016519446@192.168.5.55,
SIP        Status: 100 Trying
SIP/SDP    Request: INVITE sip:12016519446@spscom.com, w
SIP        Status: 100 Trying
SIP        Request: CANCEL sip:12016519446@192.168.5.55
```

```
⊞ Fra
⊞ Eth
⊞ Int
⊞ Tra
⊞ [Re
⊟ Ses
  ⊟ R
  ⊟ M
    ⊞ CSeq: 1 INVITE
      Max-Forwards: 70
      Route: <sip:192.168.5.55;lr;phase=terminating;transport=tcp>
      Record-Route: <sip:192.168.5.5;lr;transport=tcp>
    ⊞ Via: SIP/2.0/TCP 192.168.5.5;branch=z9hG4bK0925afe6dfadc1b91047ea14c900
      User-Agent: Avaya CM/R015x.00.0.825.4
      Supported: 100rel, timer, replaces, join, histinfo
      Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO, PUBLISH
    ⊞ Contact: "Chris Clauss" <sip:9733598557@192.168.5.5;transport=tcp>
      Session-Expires: 1800;refresher=uac
```

We need to protect voice call and signalling

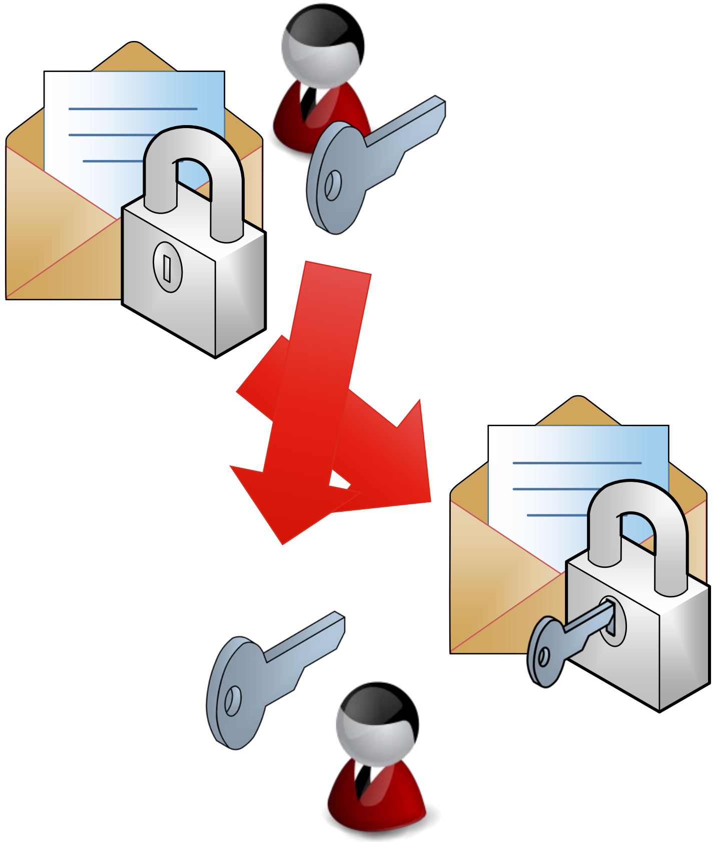
We can protect voice calls using encryption.

TLS based encryption of SIP and h.323 signaling

Secure RTP (SRTP) of the media path.

We use encryption to protect data.
Lock data – unlock with a key

- The sender encrypts the data with a key.
- The receiver uses the key to unlock the data.
- This is symmetric encryption – both sides use the same key.
- Problem is key distribution. How can we share the keys in a secure fashion?



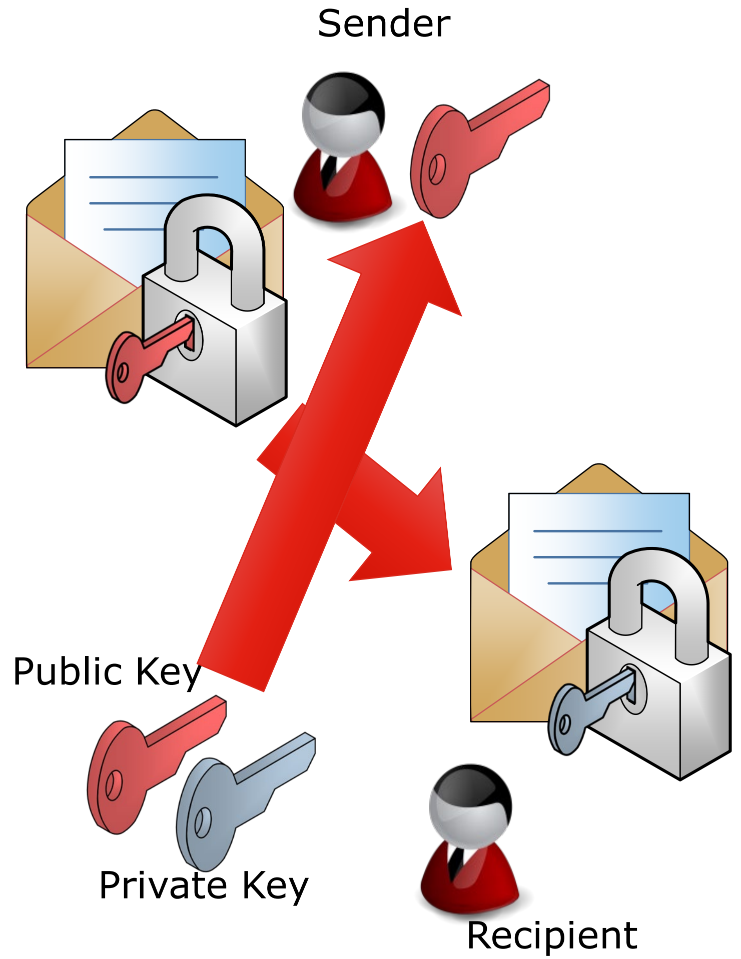
We use encryption to protect data.
Public Key Encryption

Instead of sending a key, we send a lock. Only the recipient has the key to unlock the data.

Based on mathematic formulas that create a key pair. One private and one public.

Data encrypted with one key can be decrypted with another.

Send uses public key to encrypt data, receiver uses private key to decrypt.

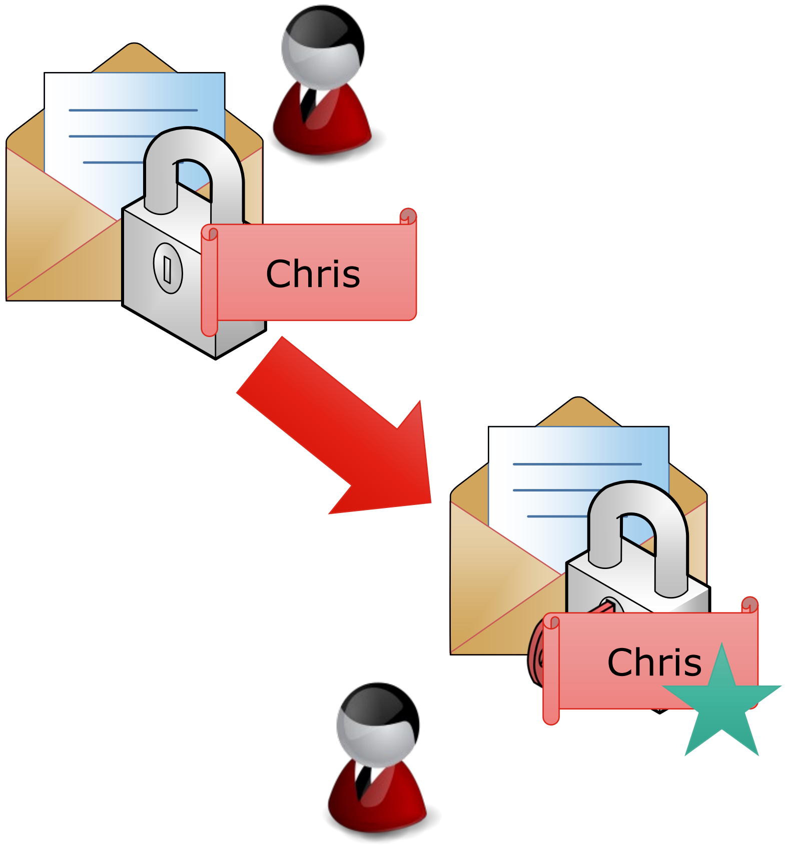


Encryption provides confidentiality, but does not provide authentication.

To provide authentication, the sender can “sign” the data with their own private key. This is the senders certificate.

The receiver can decrypt the signature using the sender’s public key.

Problem remains, how can we be sure the sender is who they say they are?



So, what is a Certificate Authority

A trusted source of Certificates.

- This can be a public company such as GoDaddy / GlobalSign / SSL.COM
- It can be a private service your company hosts using software such as Microsoft Active Directory Certificate Services or Java Certificate Authority (EJBCA)
- In an Avaya Aura Solution, System Manager can be used as a certificate authority. SMGR leverages EJBCA

The certificate authority is responsible for issuing certificates. If you trust the certificate authority, your trust the certificates.

A simple example of certificate issued by some authorities. Would you trust…?

Certificate trusted universally because we trust the US Government to issue valid passports with security features to prevent counterfeiting.

Company Name

☎ +0 123 658 944

+0 123 658 644

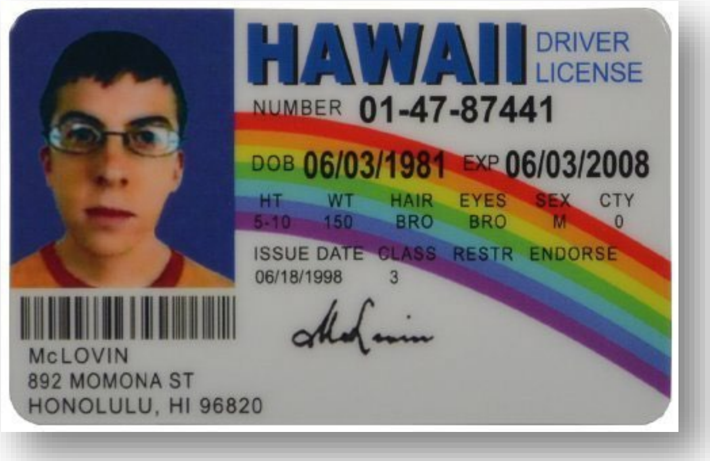
name@ companyname.com

www. companyname.com

Your company Address

Your Name
Job Position

Trusted withing an organization. May or may not be trusted outside unless there is a relationship.



HAWAII DRIVER LICENSE

NUMBER 01-47-87441

DOB 06/03/1981 EXP 06/03/2008

HT	WT	HAIR	EYES	SEX	CTY
5-10	150	BRO	BRO	M	0

ISSUE DATE	CLASS	RESTR	ENDORSE
06/18/1998	3		

McLOVIN
892 MOMONA ST
HONOLULU, HI 96820

Would you trust this "certificate"? Why or why not?

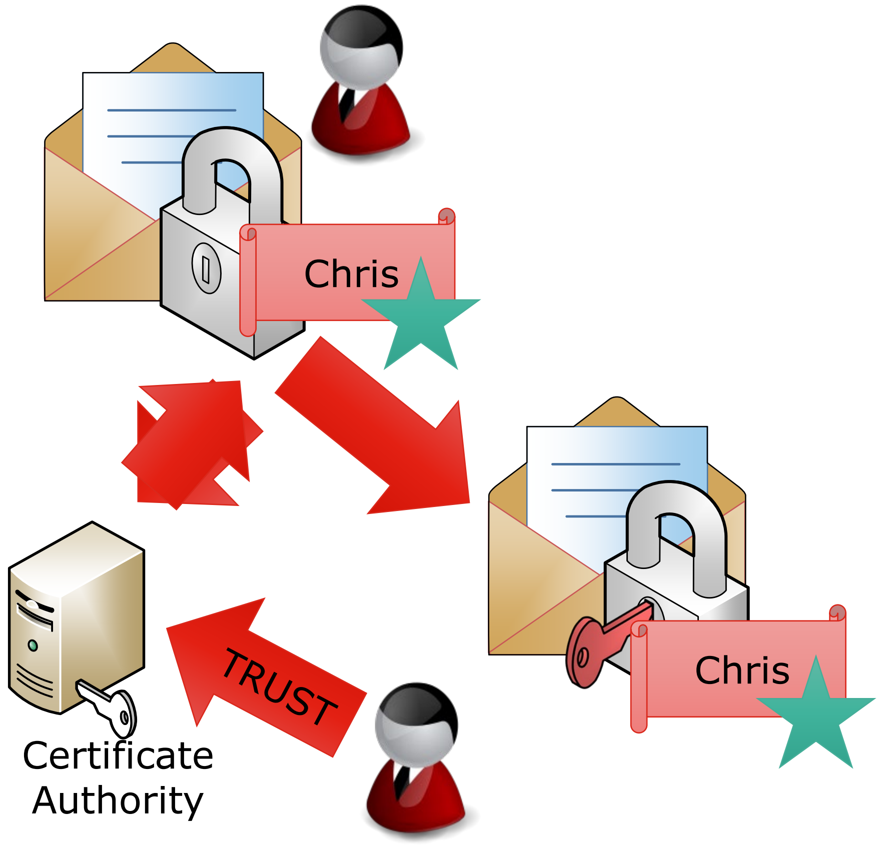
Use a certificate authority to certify the identity of the sender…

The sender sends a copy of the certificate to a certificate authority (CA).

The certificate authority signs the senders certificate, and establishes a chain of trust.

Since we trust the CA, and the sender’s data was signed by a certificate trusted by the CA, we trust the data.

This is the “chain of trust”.

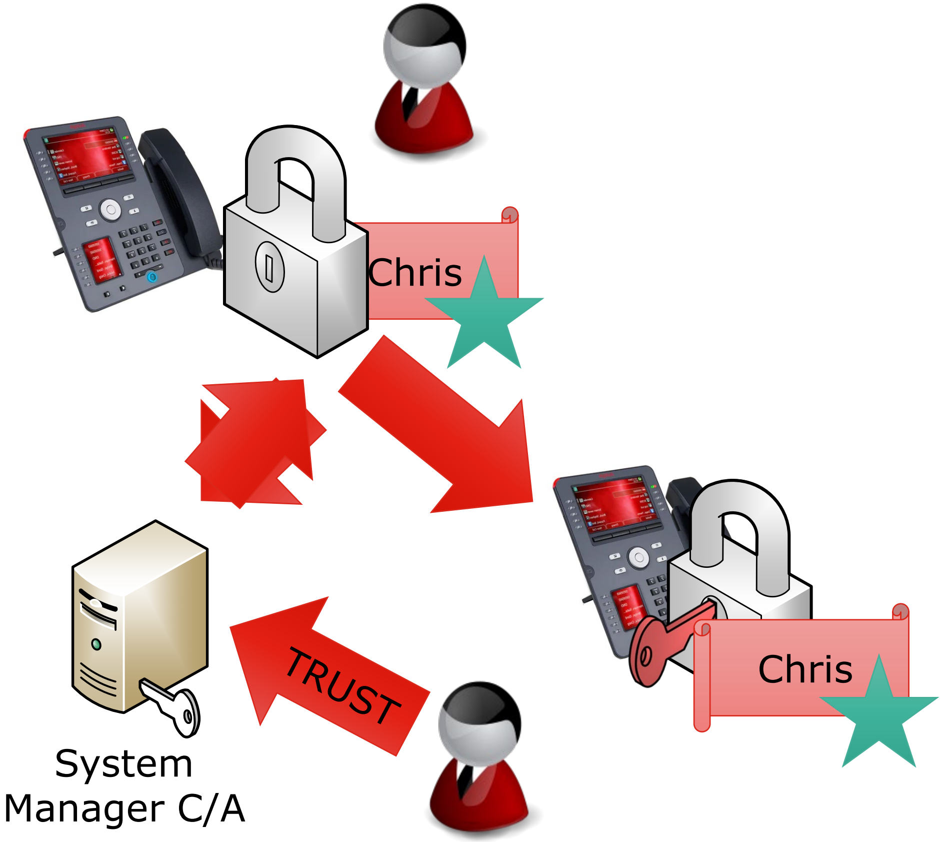


In an Avaya Infrastructure System Manager can be the “CA”

System Manager can serve as the certificate authority for Avaya servers.

System Manager provides signed certificates for Session Manager, CM, SBC, etc.

Customers can use a public CA. In this case System Manager becomes a subordinate CA.



Three types of Certificates

Root / Trusted Certificates (and also intermediate certs).

- Certificate that validates the Certificate Authority itself (GoDaddy / System Manager). A root certificate is self signed, and keys are very secure.

Server / Identity Certificates

- Signed by a Root Certificate Authority
- Systems will trust the server / identity certificate if the system trusts the root.

Self Signed Certificate

- A certificate created by a server itself. Any other server that needs to trust this machine must also install this self signed cert in the server's trust store.

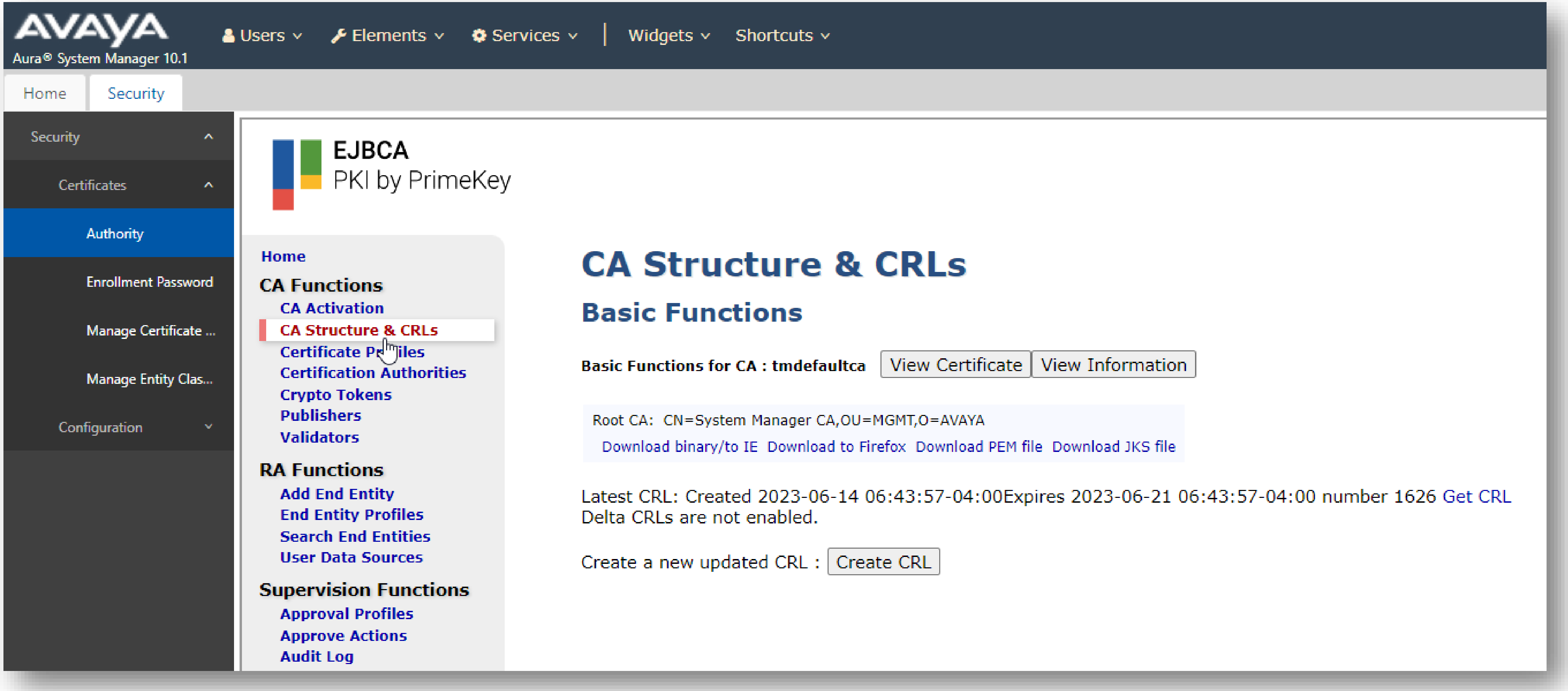
How to get Certificates for a server?

Certificates can be requested from a certificate authority two ways. Recall that for public key encryption, two keys are needed – a private key and a public key.

Create a certificate signing request. This will create our keys and creates and unsigned certificate in a request. This request is sent to the CA to be signed. We can now install this signed certificate to be used by the server.

Have the CA create the keys and certificate. This will generate a password protected file with the two keys and a signed certificate that can be installed an used by the server.

System Manager Certificate Authority



CA Structure & CRLs

Basic Functions

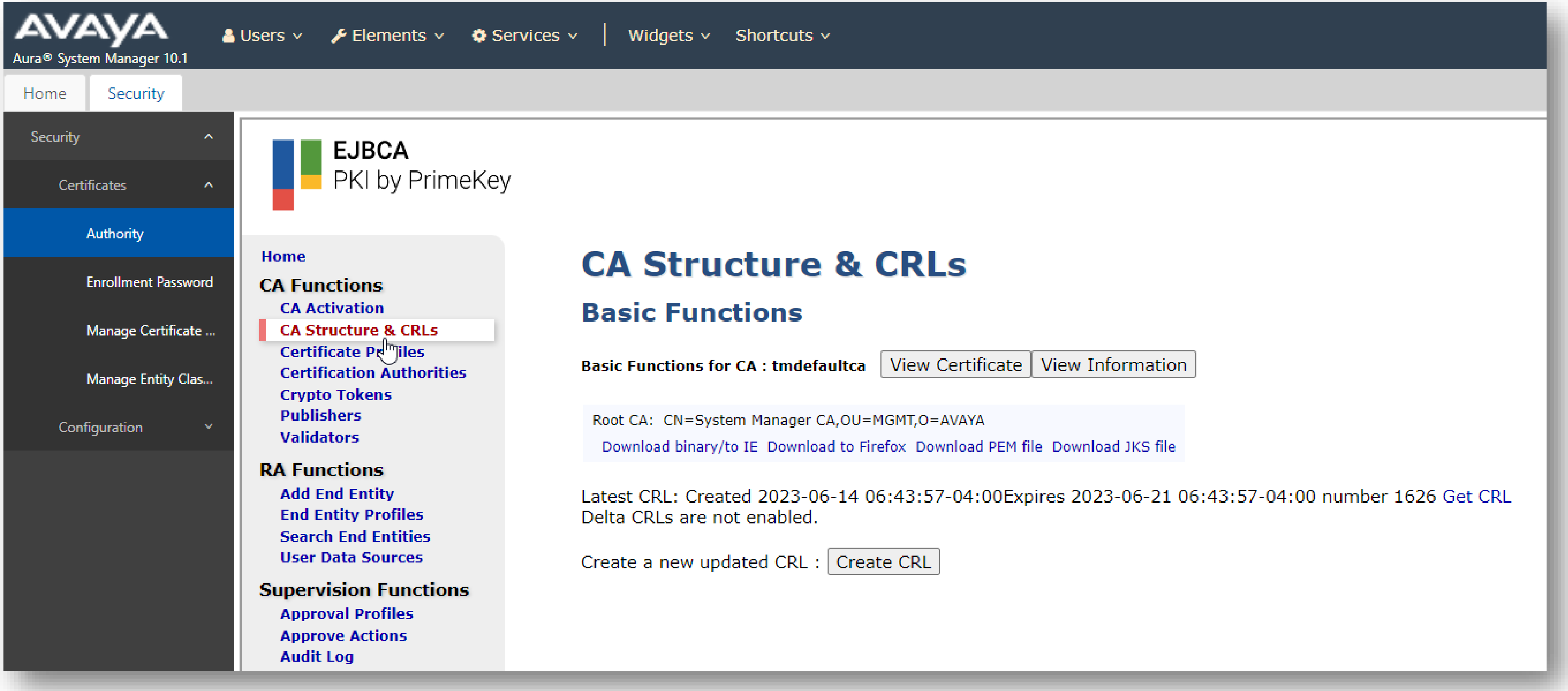
Basic Functions for CA : tmdefaultca View Certificate View Information

Root CA: CN=System Manager CA,OU=MGMT,O=AVAYA
Download binary/to IE Download to Firefox Download PEM file Download JKS file

Latest CRL: Created 2023-06-14 06:43:57-04:00Expires 2023-06-21 06:43:57-04:00 number 1626 Get CRL
Delta CRLs are not enabled.

Create a new updated CRL : Create CRL

System Manager Certificate Authority – Viewing / Download Root



CA Structure & CRLs

Basic Functions

Basic Functions for CA : tmdefaultca View Certificate View Information

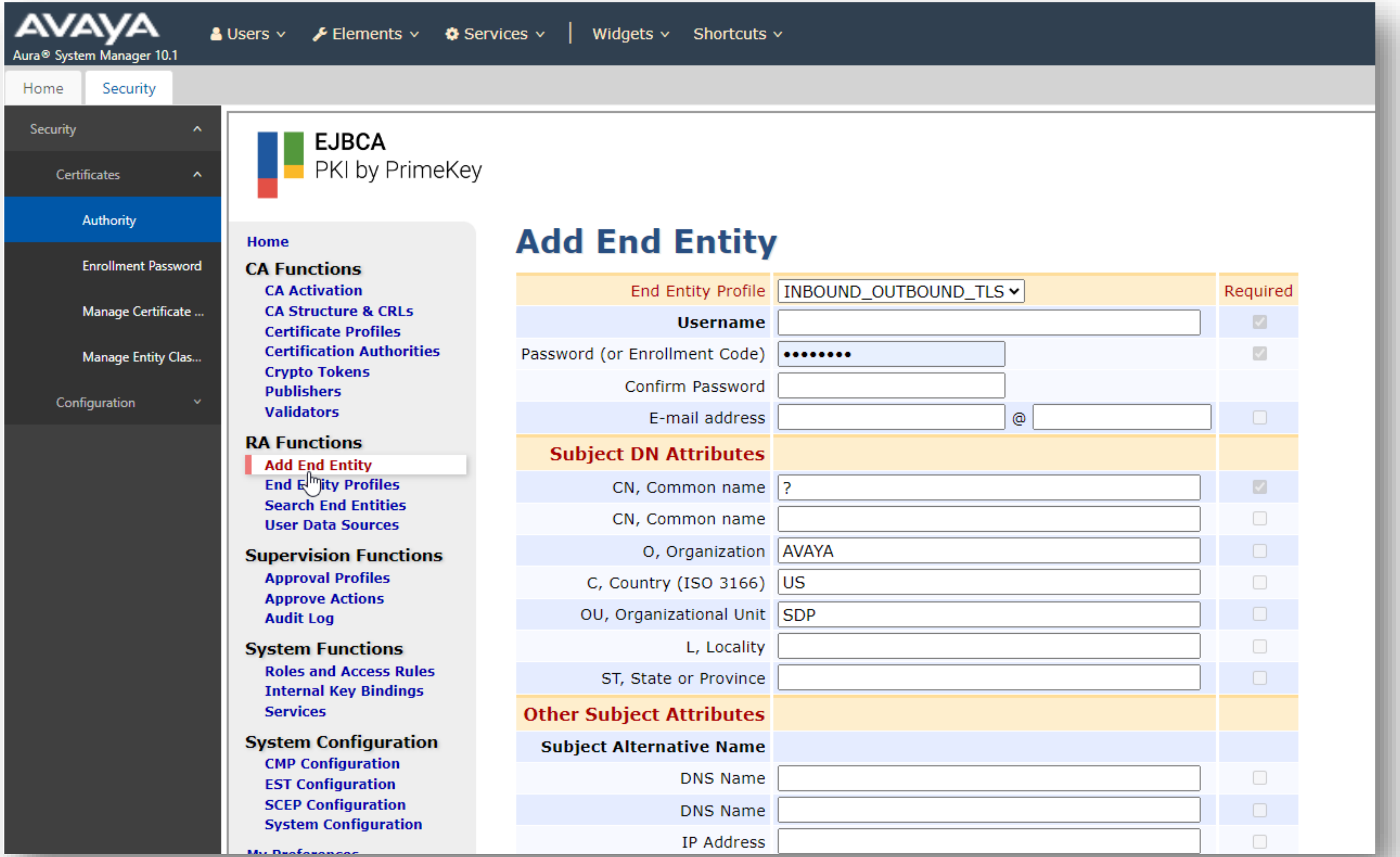
Root CA: CN=System Manager CA,OU=MGMT,O=AVAYA

Download binary/to IE Download to Firefox Download PEM file Download JKS file

Latest CRL: Created 2023-06-14 06:43:57-04:00Expires 2023-06-21 06:43:57-04:00 number 1626 Get CRL
Delta CRLs are not enabled.

Create a new updated CRL : Create CRL

System Manager Certificate Authority – Registration Authority (RA) Functions – Registers info for a certificate

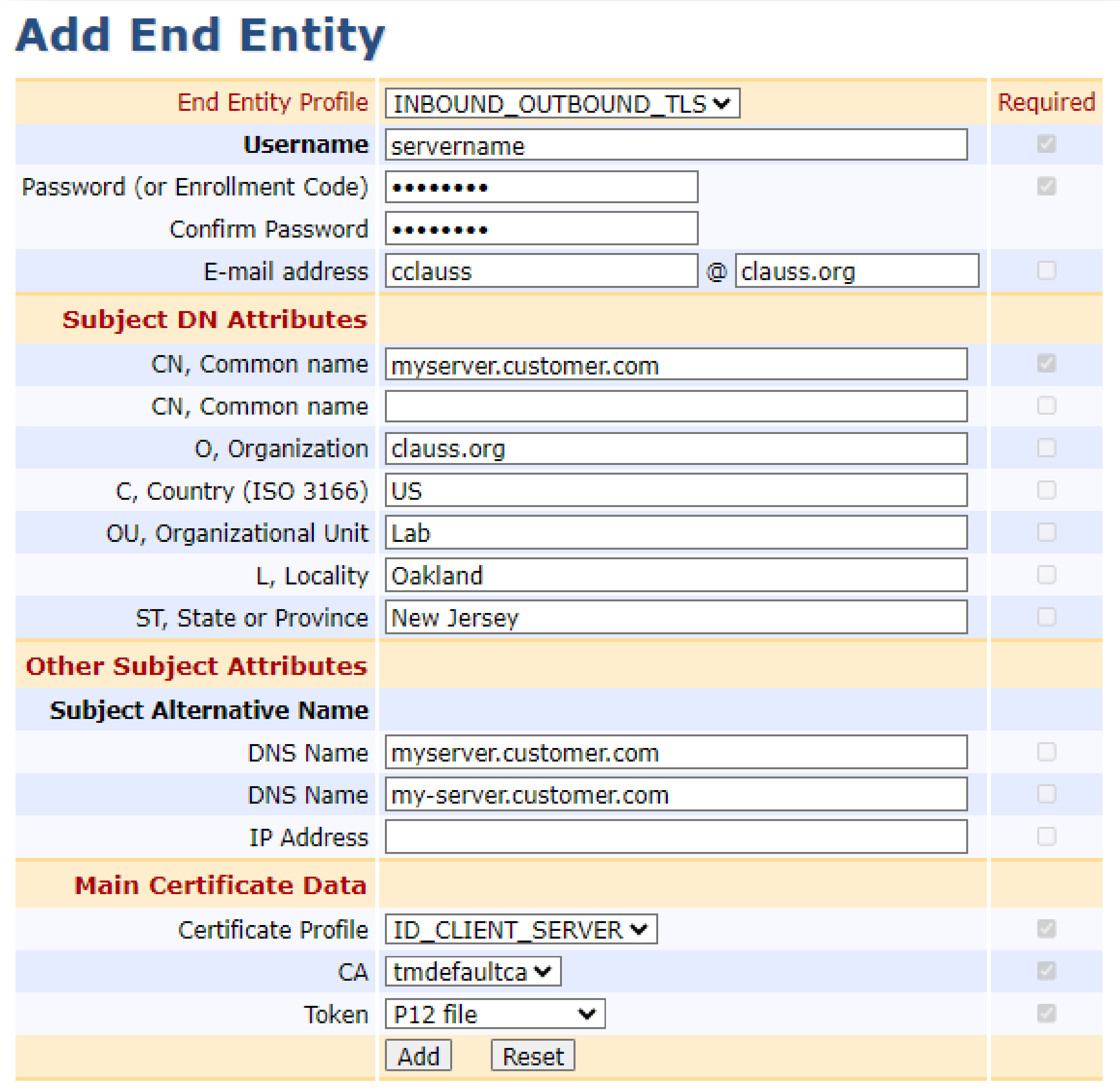


Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username		☑
Password (or Enrollment Code)	••••••••	☑
Confirm Password		
E-mail address	@	□
Subject DN Attributes		
CN, Common name	?	☑
CN, Common name		□
O, Organization	AVAYA	□
C, Country (ISO 3166)	US	□
OU, Organizational Unit	SDP	□
L, Locality		□
ST, State or Province		□
Other Subject Attributes		
Subject Alternative Name		
DNS Name		□
DNS Name		□
IP Address		□

System Manager Certificate Authority – RA Functions – Create or Sign Identity Certs for Servers

- Username – use the server name
- Password – your choice – remember it
- eMail – options
- Common Name – server DNS name
- Organization / Country / Unit / Locality / State are all optional. Informational
- Subject Alternative Name – very important.
  Specify the DNS name of the server.
  Add a secondary name if needed.
  Do not add IP address – bad practice.
  SAN is enforced by Apple and Google since 2018.
- Select the Token Type



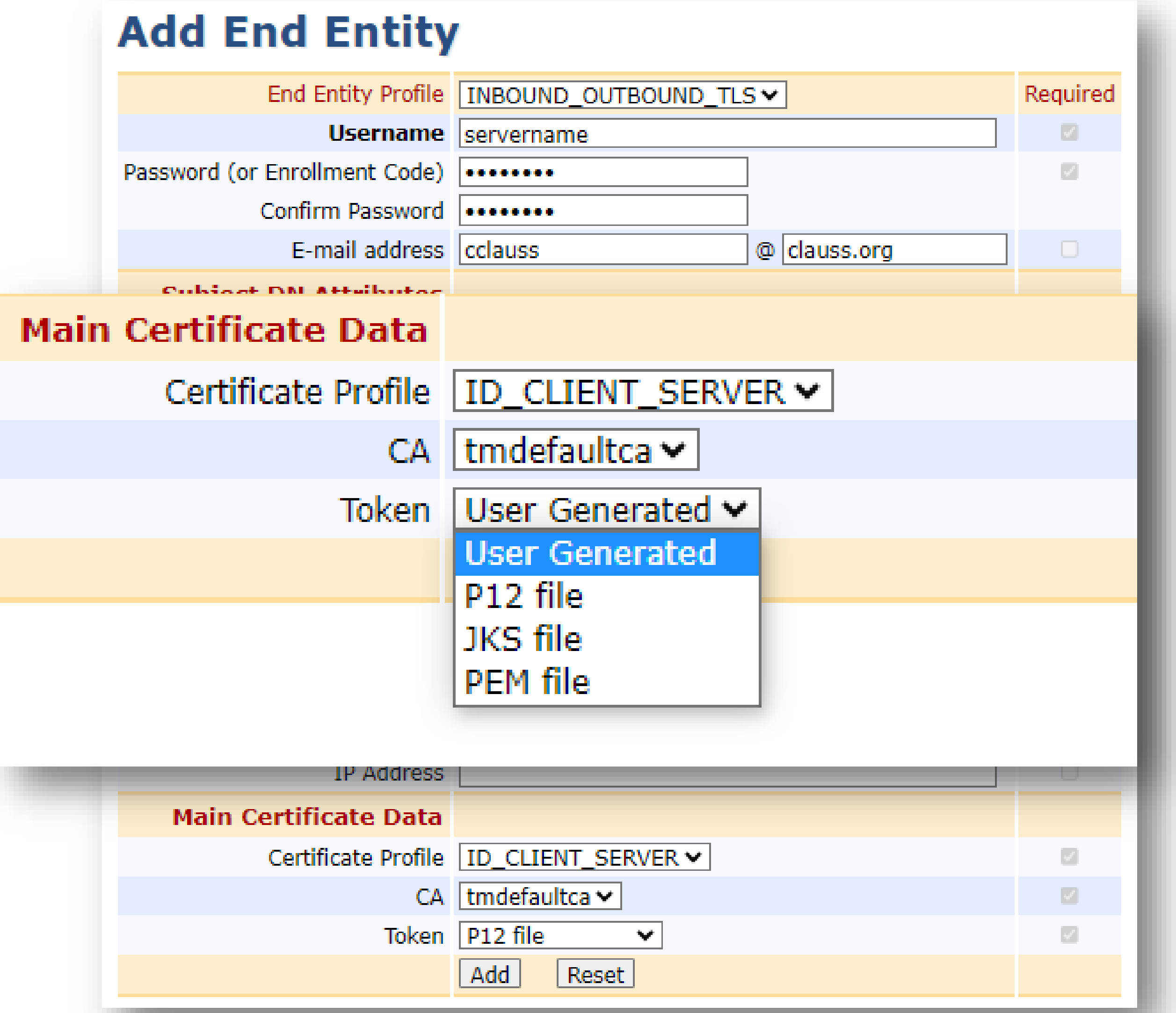
Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username	servername	☑
Password (or Enrollment Code)	••••••••	☑
Confirm Password	••••••••	
E-mail address	cclauss @ clauss.org	□
Subject DN Attributes		
CN, Common name	myserver.customer.com	☑
CN, Common name		□
O, Organization	clauss.org	□
C, Country (ISO 3166)	US	□
OU, Organizational Unit	Lab	□
L, Locality	Oakland	□
ST, State or Province	New Jersey	□
Other Subject Attributes		
Subject Alternative Name		
DNS Name	myserver.customer.com	□
DNS Name	my-server.customer.com	□
IP Address		□
Main Certificate Data		
Certificate Profile	ID_CLIENT_SERVER	☑
CA	tmdefaultca	☑
Token	P12 file	☑
	Add Reset	

System Manager Certificate Authority – RA Functions – Create or Sign Identity Certs for Servers

Main Certificate Data

- Certificate used for Client / Server interactions
- CA – the CA that is signing your certificate. By default that is "tmdefaultca" which is the default name of the System Manager
- Type of "token" to be generated
    - P12 file – the SMGR will create a password protected certificate for the server including keys
    - PEM file – the SMGR will create a simple certificate file but requires a certificate signing request from the server
- Click Add when done



Add End Entity

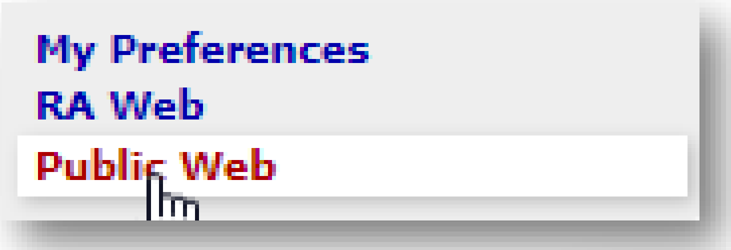
End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username	servername	☑
Password (or Enrollment Code)	••••••••	☑
Confirm Password	••••••••	
E-mail address	cclauss @ clauss.org	□
Subject DN Attributes		
IP Address		□
Main Certificate Data		
Certificate Profile	ID_CLIENT_SERVER	☑
CA	tmdefaultca	☑
Token	P12 file	☑
	Add Reset	

Main Certificate Data

Certificate Profile	ID_CLIENT_SERVER
CA	tmdefaultca
Token	User Generated

We added a registration, and now need to create a certificate.

Select Public Web

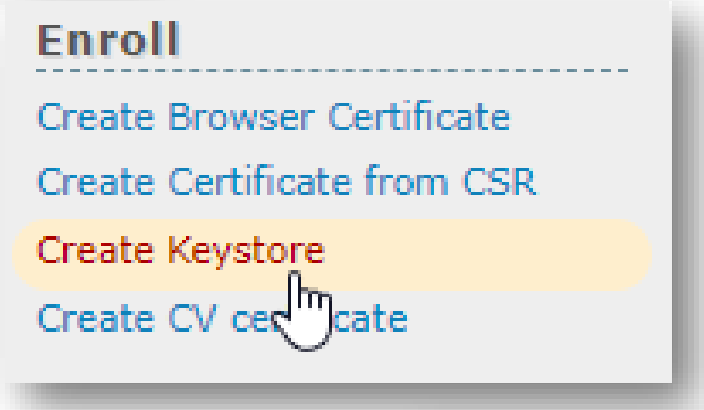


My Preferences

RA Web

Public Web

To generate a new cert with keys, select the option to Create a Keystore.



Enroll

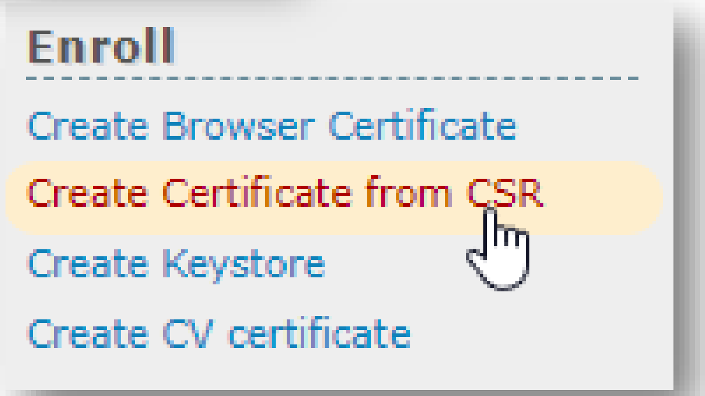
Create Browser Certificate

Create Certificate from CSR

Create Keystore

Create CV certificate

To generate a new cert in response to a signing request, select Create Certificate from CSR.



Enroll

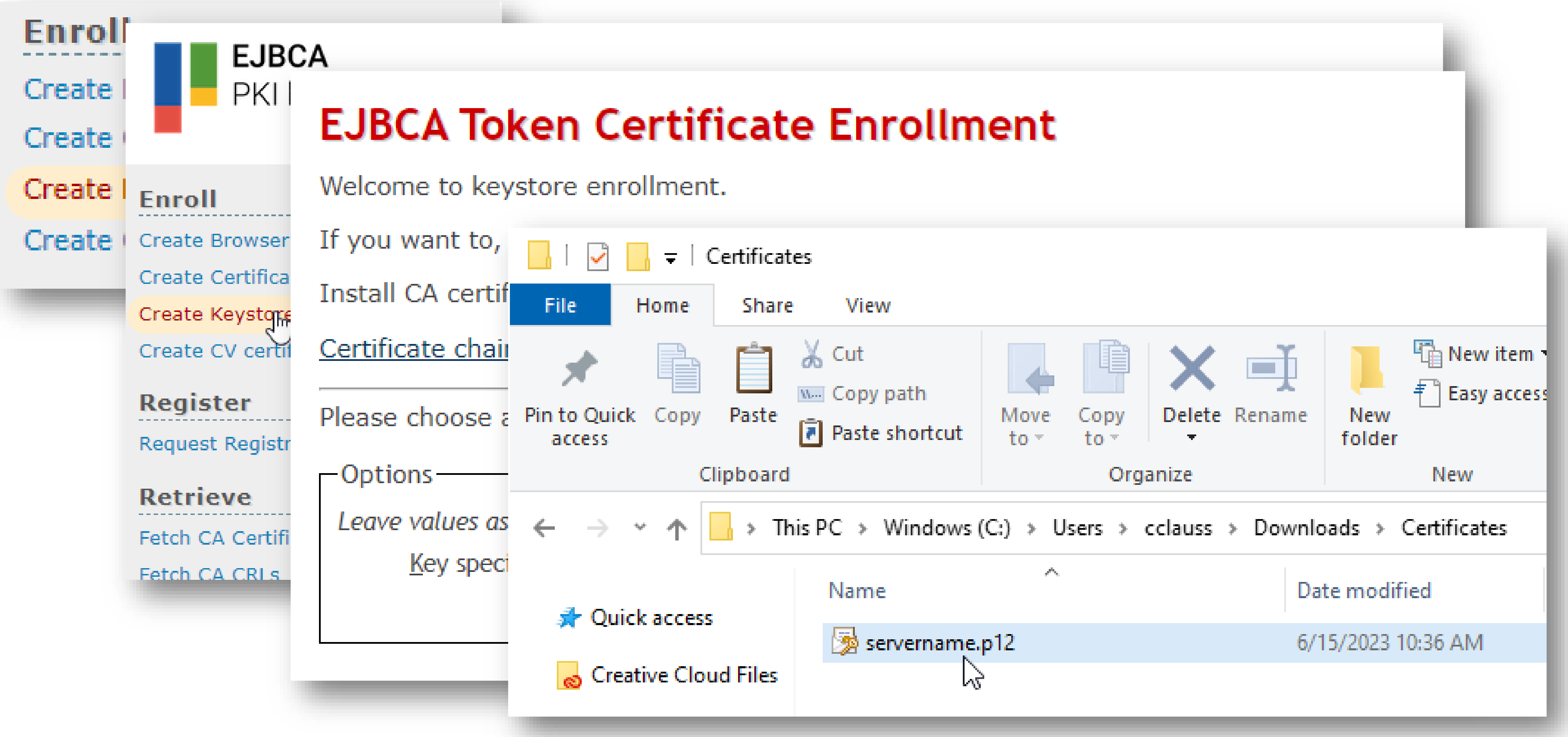
Create Browser Certificate

Create Certificate from CSR

Create Keystore

Create CV certificate

Creating the certificate for the registered earlier…



Enroll
Create
Create
Create
Create

EJBCA
PKI

Enroll
Create Browser
Create Certifica
Create Keystore
Create CV certi

Register
Request Registr

Retrieve
Fetch CA Certifi
Fetch CA CRLs

EJBCA Token Certificate Enrollment

Welcome to keystore enrollment.

If you want to,

Install CA certif

Certificate chai

Please choose a

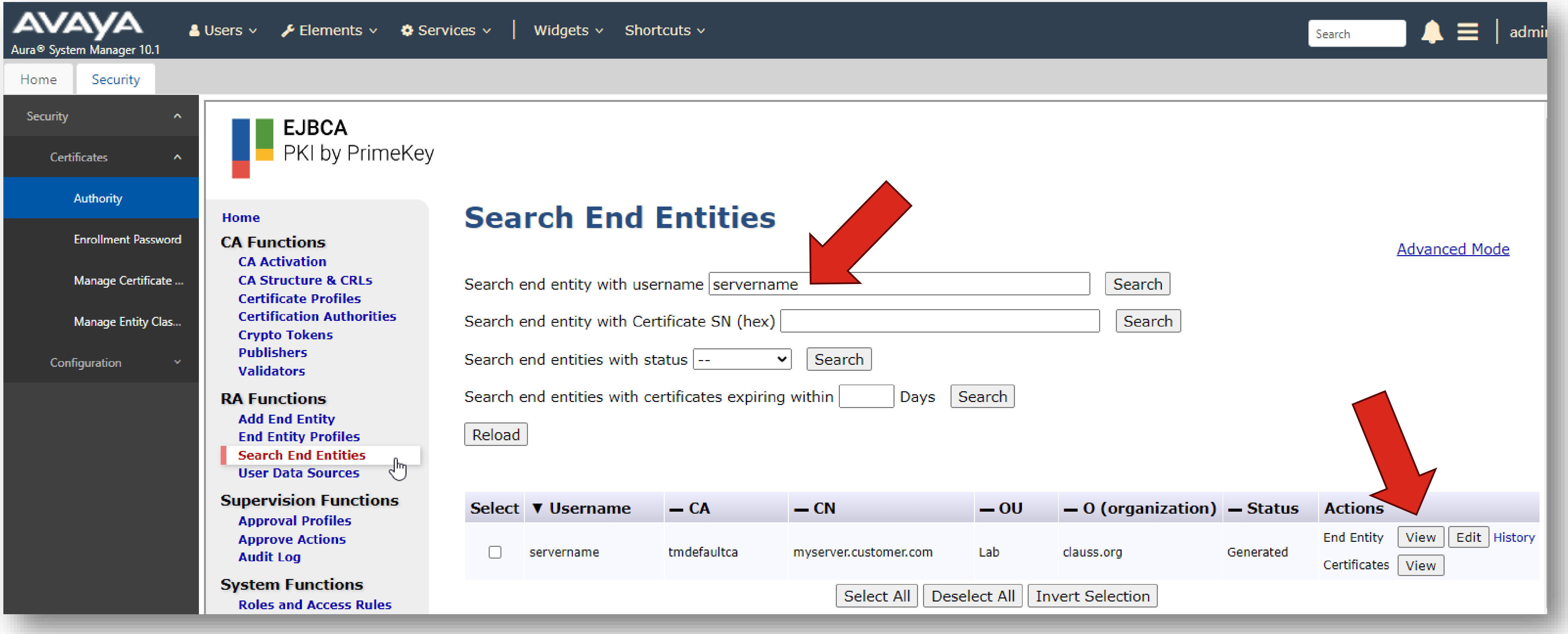
Options

Leave values as

Key speci

Name	Date modified
servername.p12	6/15/2023 10:36 AM

Viewing the Certificate in System Manager



Search End Entities

Advanced Mode

Search end entity with username servername [Search]

Search end entity with Certificate SN (hex) [Search]

Search end entities with status -- [Search]

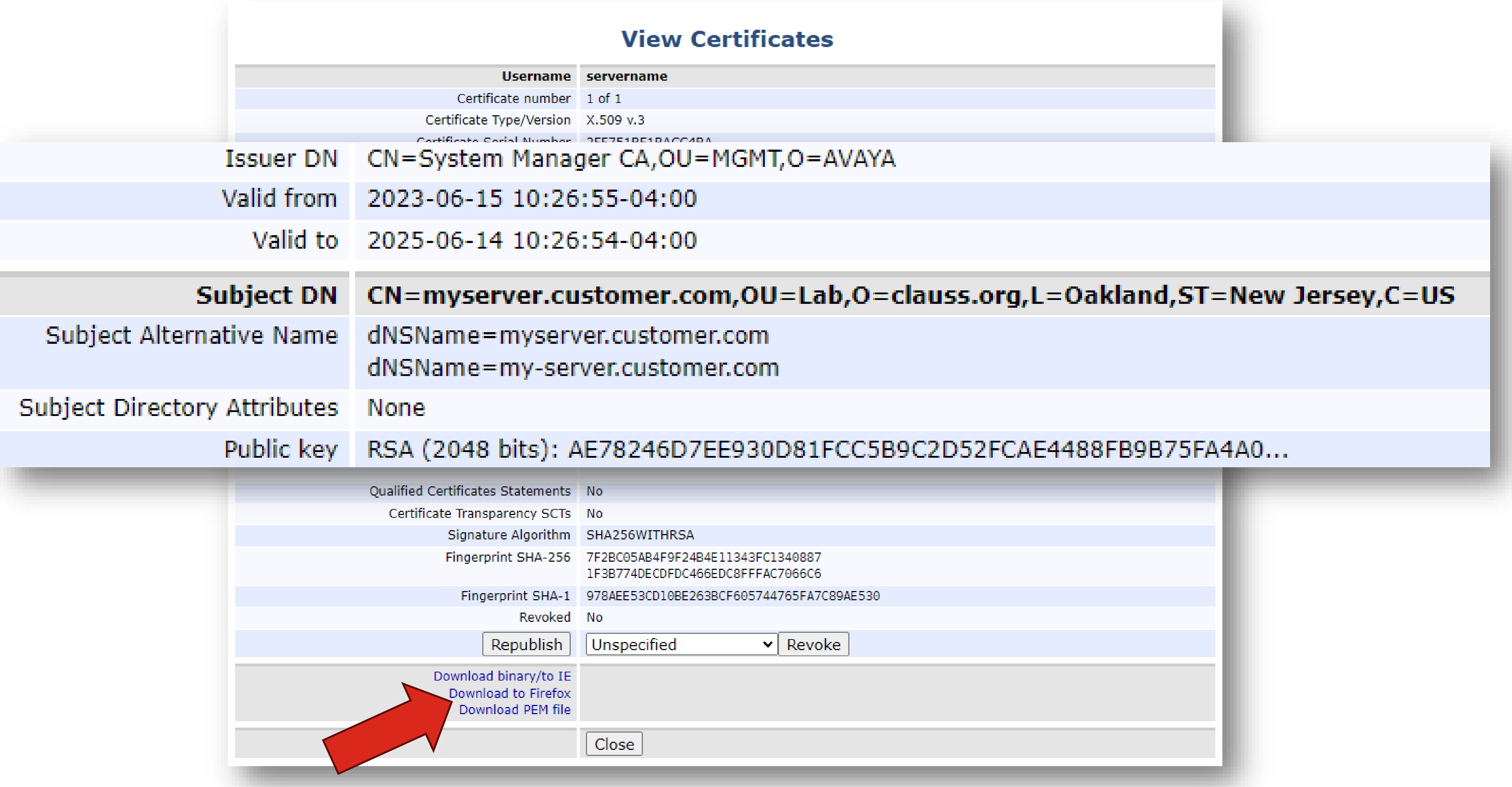
Search end entities with certificates expiring within ___ Days [Search]

[Reload]

Select	▼ Username	— CA	— CN	— OU	— O (organization)	— Status	Actions
□	servername	tmdefaultca	myserver.customer.com	Lab	clauss.org	Generated	End Entity [View] [Edit] History Certificates [View]

[Select All] [Deselect All] [Invert Selection]

Viewing the Certificate in System Manager



View Certificates

Username	**servername**
Certificate number	1 of 1
Certificate Type/Version	X.509 v.3
Certificate Serial Number	2FF751BF1BACC4BA
Issuer DN	CN=System Manager CA,OU=MGMT,O=AVAYA
Valid from	2023-06-15 10:26:55-04:00
Valid to	2025-06-14 10:26:54-04:00
Subject DN	**CN=myserver.customer.com,OU=Lab,O=clauss.org,L=Oakland,ST=New Jersey,C=US**

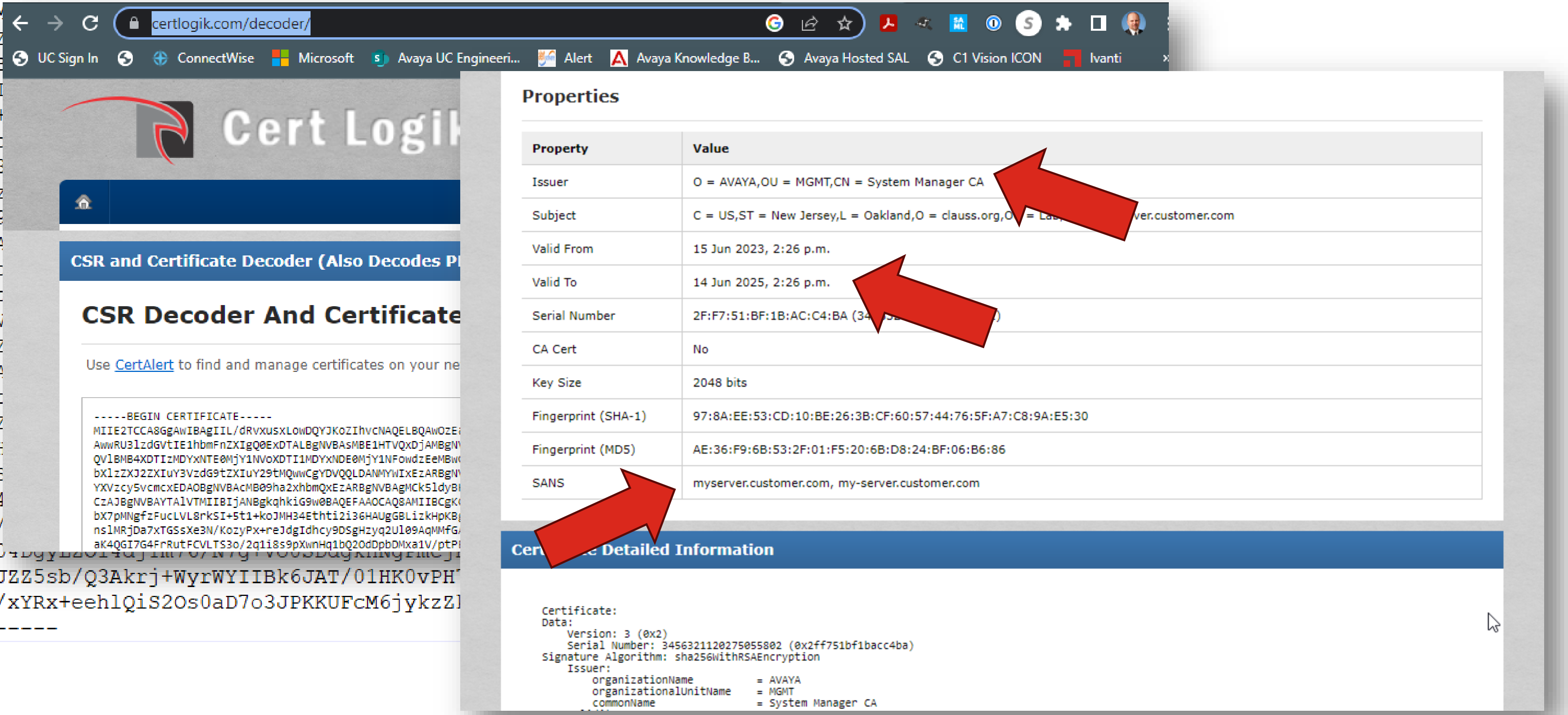
Subject Alternative Name	dNSName=myserver.customer.com
	dNSName=my-server.customer.com

Subject Directory Attributes	None
Public key	RSA (2048 bits): AE78246D7EE930D81FCC5B9C2D52FCAE4488FB9B75FA4A0...
Qualified Certificates Statements	No
Certificate Transparency SCTs	No
Signature Algorithm	SHA256WITHRSA
Fingerprint SHA-256	7F2BC05AB4F9F24B4E11343FC1340887 1F3B774DECDFDC466EDC8FFFAC7066C6
Fingerprint SHA-1	978AEE53CD10BE263BCF605744765FA7C89AE530
Revoked	No
Republish	Unspecified ⌄ Revoke
Download binary/to IE Download to Firefox Download PEM file	
	Close

Looking at a certificate file – copy and paste your cert to an online decoder…

https://certlogik.com/decoder/

```
-----BEGIN CERTIFICATE-----
MIIE2TCCA8GgAwIBAgIIL/dRvxusxLowDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UE
AwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFW
QVlBMB4XDTIzMDYxNTE0M
bXlzZXJ2ZXIuY3VzdG9tZ
YXVzcy5vcmcxEDAOBgNVB
CzAJBgNVBAYTAlVTMIIBI
bX7pMNgfzFucLVL8rkSI+
nslMRjDa7xTGSsXe3N/Ko
aK4QGI7G4FrRutFCVLTS3
r3hBXIpHf74CaJmY8XHBz
G+Gy+xU8ipdf8fI11kOV9
Yo2WPeJIgM/K3YwMqQIDA
GDAWgBRYMhsdiKRJE1sqc
BQUHMAGGNGh0dHA6Ly9nc
c3RhdHVzL29jc3AwOAYDV
eS1zZXJ2ZXIuY3VzdG9tZ
FAYIKwYBBQUHAwEGCCsGA
Z3JzbWdyLmNsYXVzcy5vc
c3Q/Y21kPWNybCZpc3N1Z
TVQsTz1BVkFZQTAdBgNVH
AQH/BAQDAgP4MA0GCSqGS
zXaGzuKyFPJvMQXsGmIK4
y65wBa5sJsMWpyX8QMSP/
0ssoMX164uKl3PKADC4Z0
m13pEZk56MdXLyrqhnLxJZZ5sb/Q3Akrj+WyrWYIIBk6JAT/01HK0vPHT
M45UJ4irB0Bm1yu10ubK/xYRx+eehlQiS2Os0aD7o3JPKKUFcM6jykzZl
-----END CERTIFICATE-----
```



CSR and Certificate Decoder (Also Decodes P

CSR Decoder And Certificate

Use CertAlert to find and manage certificates on your ne

```
-----BEGIN CERTIFICATE-----
MIIE2TCCA8GgAwIBAgIIL/dRvxusxLowDQYJKoZIhvcNAQELBQAwOzEa
AwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNV
QVlBMB4XDTIzMDYxNTE0MjY1NVoXDTI1MDYxNDE0MjY1NFowdzEeMBw
bXlzZXJ2ZXIuY3VzdG9tZXIuY29tMQwwCgYDVQQLDANMYWIxEzARBgNV
YXVzcy5vcmcxEDAOBgNVBAcMB09ha2xhbmQxEzARBgNVBAgMCk5ldyB
CzAJBgNVBAYTAlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK
bX7pMNgfzFucLVL8rkSI+5t1+koJMH34Ethti2i36HAUgGBLizkHpKB
nslMRjDa7xTGSsXe3N/KozyPx+reJdgIdhcy9DSgHzyq2Ul09AqMMfG
aK4QGI7G4FrRutFCVLTS3o/2q1i8s9pXwnHq1bQ2OdDpbDMxa1V/ptP
```

Properties

Property	Value
Issuer	O = AVAYA,OU = MGMT,CN = System Manager CA
Subject	C = US,ST = New Jersey,L = Oakland,O = clauss.org,O = La ver.customer.com
Valid From	15 Jun 2023, 2:26 p.m.
Valid To	14 Jun 2025, 2:26 p.m.
Serial Number	2F:F7:51:BF:1B:AC:C4:BA (34)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	97:8A:EE:53:CD:10:BE:26:3B:CF:60:57:44:76:5F:A7:C8:9A:E5:30
Fingerprint (MD5)	AE:36:F9:6B:53:2F:01:F5:20:6B:D8:24:BF:06:B6:86
SANS	myserver.customer.com, my-server.customer.com

Cer e Detailed Information

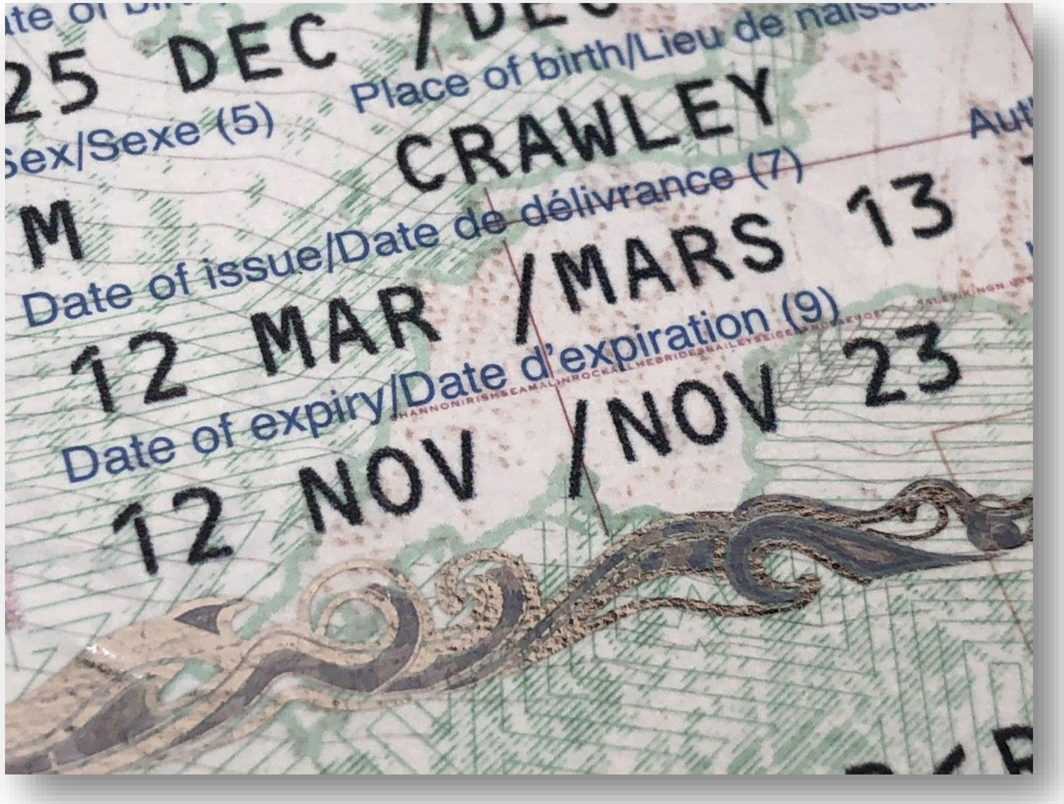
```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number: 3456321120275055802 (0x2ff751bf1bacc4ba)
Signature Algorithm: sha256WithRSAEncryption
    Issuer:
        organizationName          = AVAYA
        organizationalUnitName    = MGMT
        commonName                = System Manager CA
```

Nothing lasts forever – certificates expire…

When certificates expire, they must be replaced, just like a driver's license or a passport.

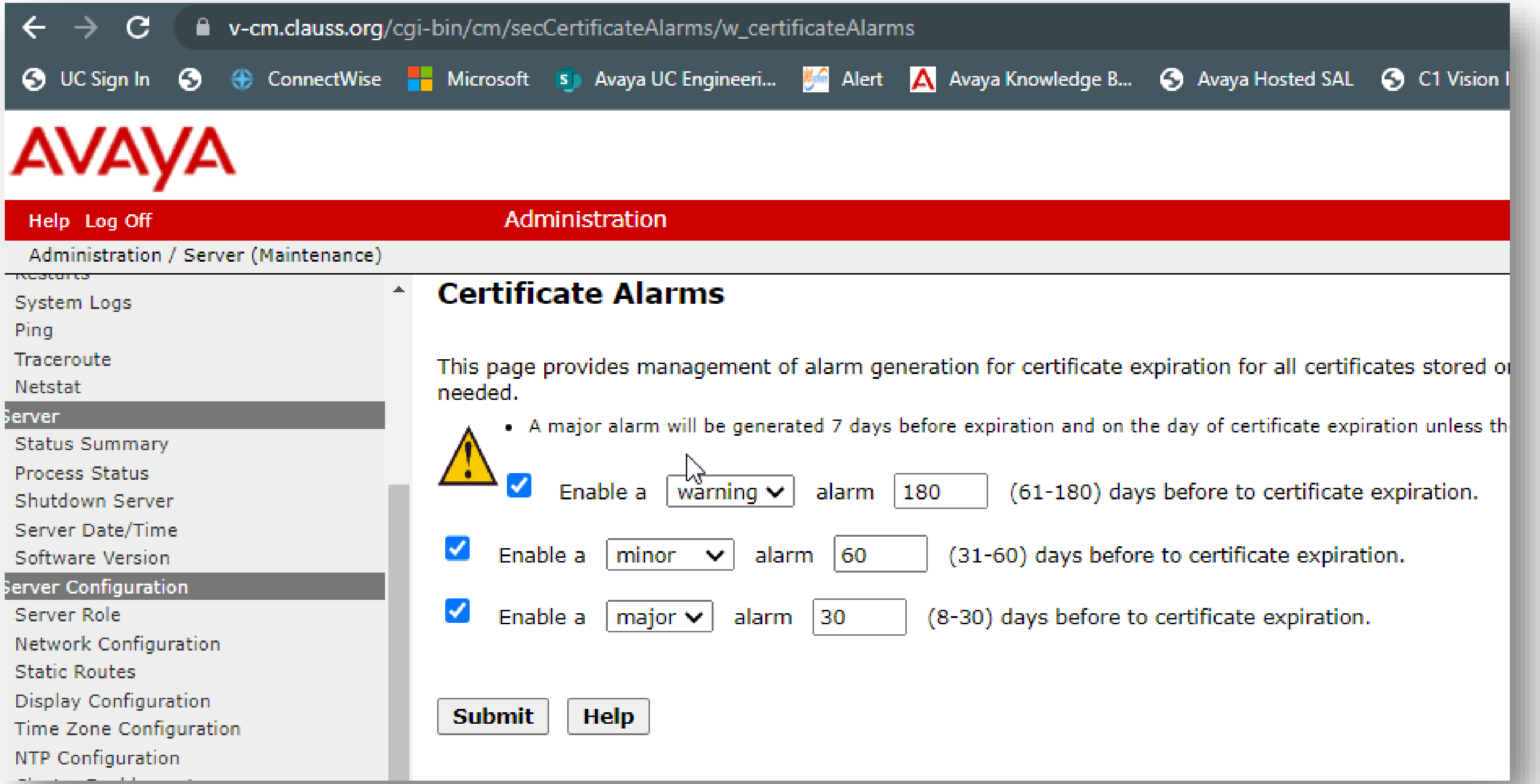
It is important to know when certs expire.

Avaya devices send alarms indicating that certificates will expire within a give number of days.


25 DEC
Sex/Sexe (5)
Place of birth/Lieu de naissance
M
CRAWLEY
Date of issue/Date de délivrance (7)
12 MAR /MARS 13
Date of expiry/Date d'expiration (9)
12 NOV /NOV 23

Nothing lasts forever – certificates expire…

Avaya devices send alarms indicating that certificates will expire within a give number of days. When certs expire, things stop working.



Certificate Alarms

This page provides management of alarm generation for certificate expiration for all certificates stored o needed.

- A major alarm will be generated 7 days before expiration and on the day of certificate expiration unless th

☑ Enable a warning alarm 180 (61-180) days before to certificate expiration.

☑ Enable a minor alarm 60 (31-60) days before to certificate expiration.

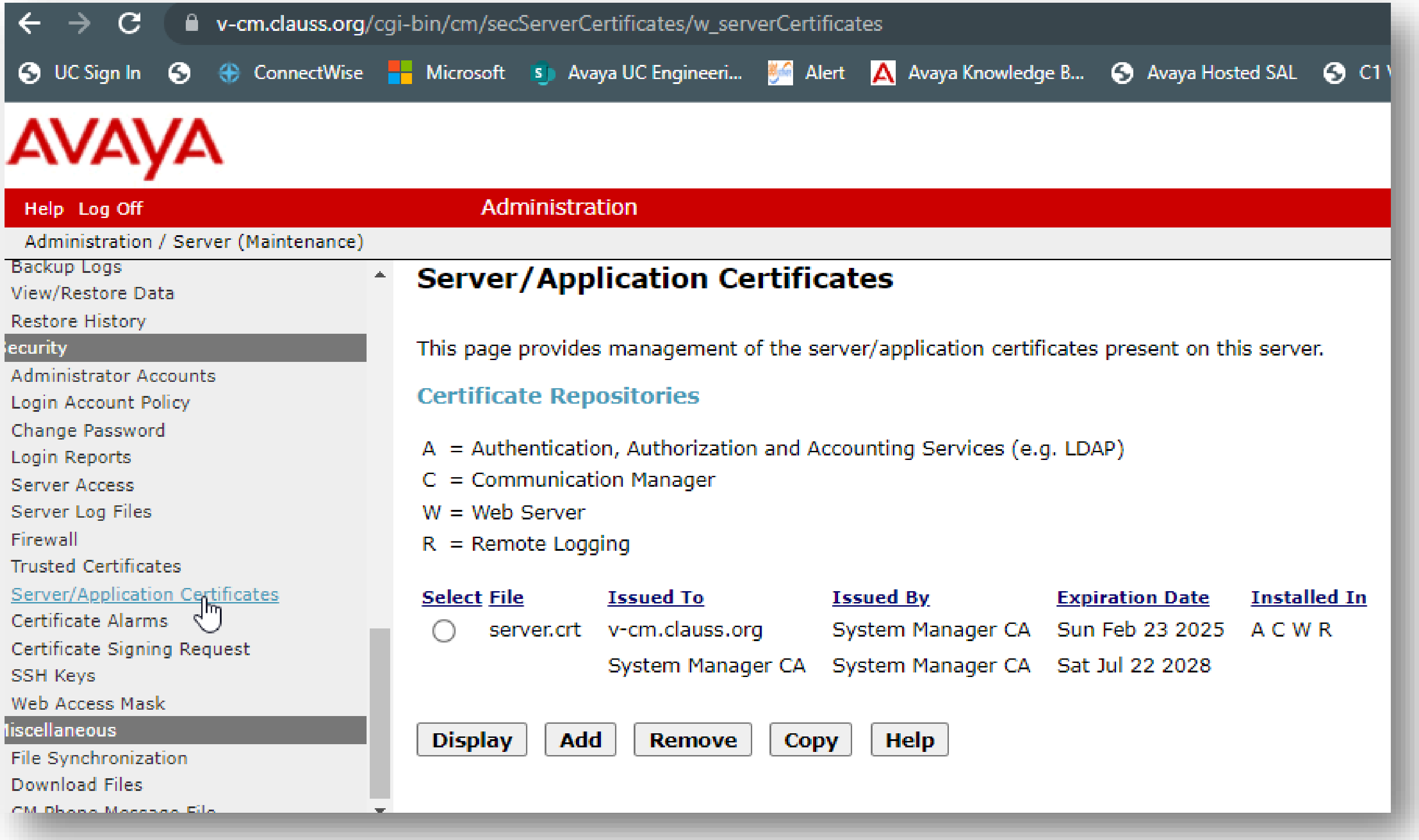
☑ Enable a major alarm 30 (8-30) days before to certificate expiration.

Submit Help

How can I find out when my certificates expire?

Look at the certificate. Certs can be viewed on the servers they are installed on.

Each product is different.



Server/Application Certificates

This page provides management of the server/application certificates present on this server.

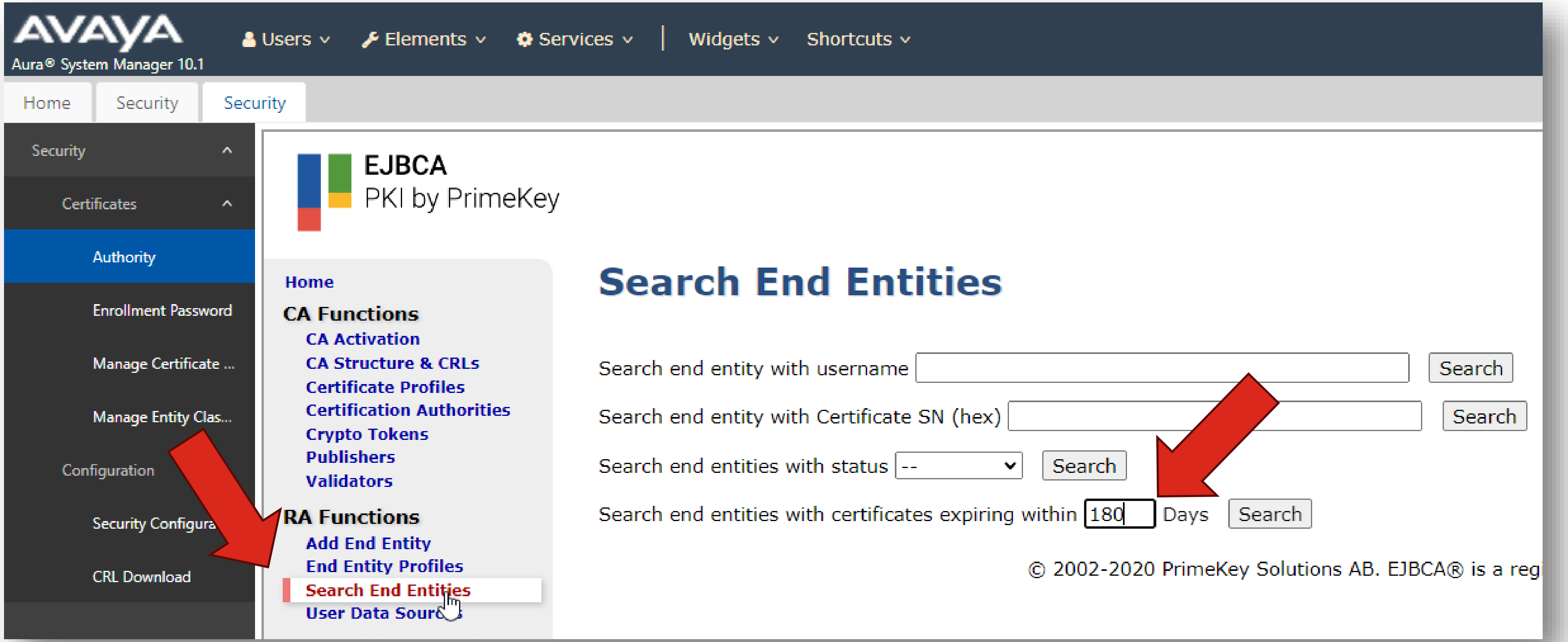
Certificate Repositories

A = Authentication, Authorization and Accounting Services (e.g. LDAP)
C = Communication Manager
W = Web Server
R = Remote Logging

Select	File	Issued To	Issued By	Expiration Date	Installed In
○	server.crt	v-cm.clauss.org	System Manager CA	Sun Feb 23 2025	A C W R
		System Manager CA	System Manager CA	Sat Jul 22 2028	

How can I find out when my certificates expire? The best way…

Look at your certificate authority for a list of all the certs that were generated and filter on expiration…



Search End Entities

Search end entity with username [ ] Search

Search end entity with Certificate SN (hex) [ ] Search

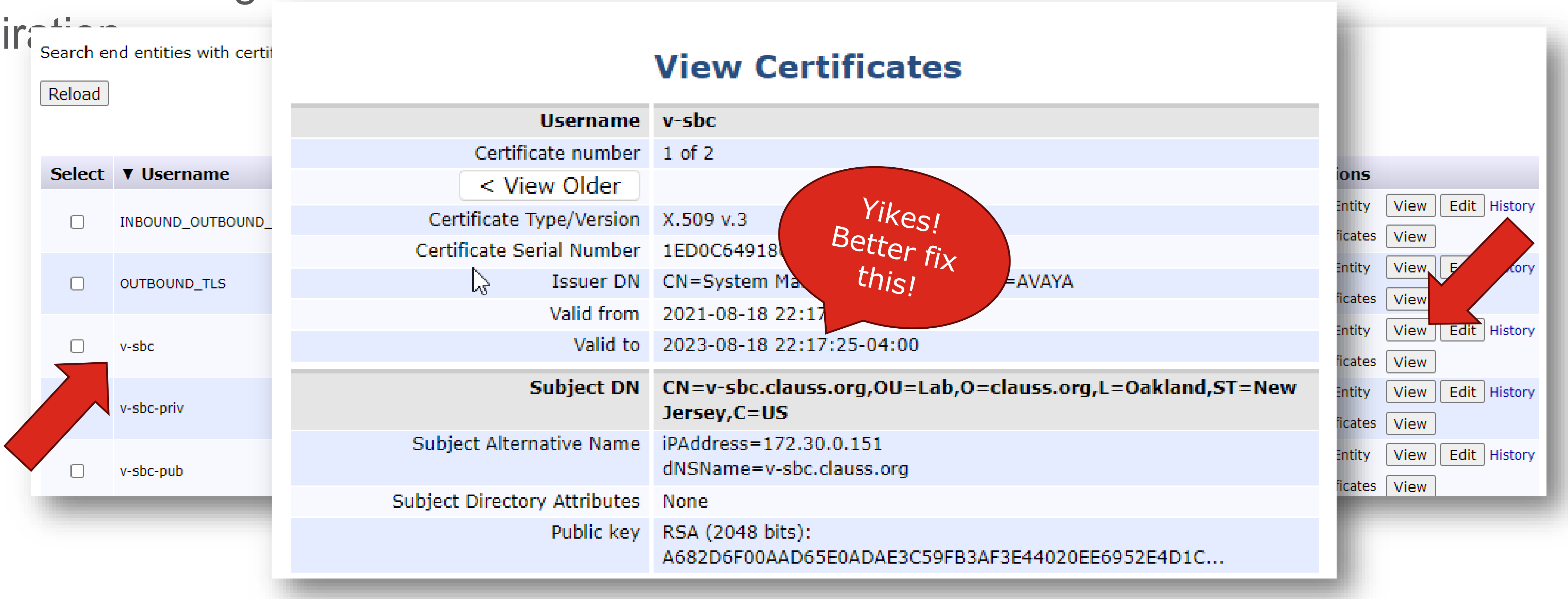
Search end entities with status [--] Search

Search end entities with certificates expiring within [180] Days Search

© 2002-2020 PrimeKey Solutions AB. EJBCA® is a reg

How can I find out when my certificates expire? The best way…

Look at your certificate authority for a list of all the certs that were generated and filter on expira



Search end entities with certi

Reload

Select	▼ Username
□	INBOUND_OUTBOUND_
□	OUTBOUND_TLS
□	v-sbc
	v-sbc-priv
□	v-sbc-pub

View Certificates

Username	v-sbc
Certificate number	1 of 2
< View Older	
Certificate Type/Version	X.509 v.3
Certificate Serial Number	1ED0C64918
Issuer DN	CN=System Ma =AVAYA
Valid from	2021-08-18 22:17
Valid to	2023-08-18 22:17:25-04:00
Subject DN	CN=v-sbc.clauss.org,OU=Lab,O=clauss.org,L=Oakland,ST=New Jersey,C=US

Subject Alternative Name	iPAddress=172.30.0.151
	dNSName=v-sbc.clauss.org

Subject Directory Attributes	None
Public key	RSA (2048 bits): A682D6F00AAD65E0ADAE3C59FB3AF3E44020EE6952E4D1C...

ions			
ntity	View	Edit	History
ficates	View		
ntity	View	E	tory
ficates	View		
ntity	View	Edit	History
ficates	View		
ntity	View	Edit	History
ficates	View		
ntity	View	Edit	History
ficates	View		

System Manager can auto renew certain certificates…

System Manager automatically renews certificates for systems in the following cases…

- System Manager is the CA that issued the certificates for the specific system.
- The system is managed by System Manager
  - Session Manager
  - Breeze
- Also, for some servers, there is an enrollment process to make renewals easier
  - Media Server
  - Avaya Aura Device Services / Web Gateway

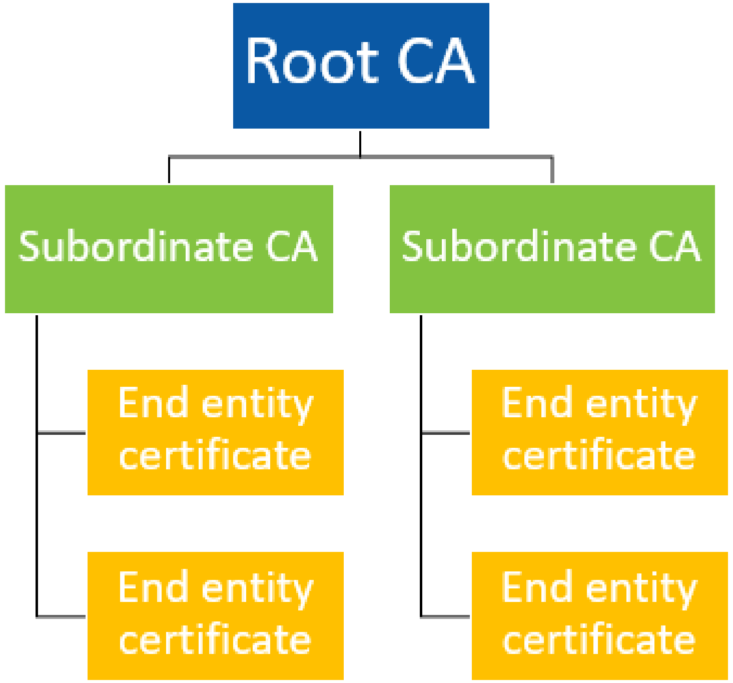
So what should we use for our Certificate Authority

Several options…

- Check with internal security team on specific company mandates.
- Use System Manager as CA for Avaya server to server communications (ease of admin and secure)
- Use Public CA for end user facing systems (SBC remote worker / web)
- Use internal CA if required.

Summary of ca hierarchy

- Root CA may be System Manager or customer CA
- Intermediate CA may or may not be used
- Each end entity will have a unique identity certificate signed by the CA.
- Each end entity must have root or intermediate certificates installed.



Root CA

Subordinate CA

Subordinate CA

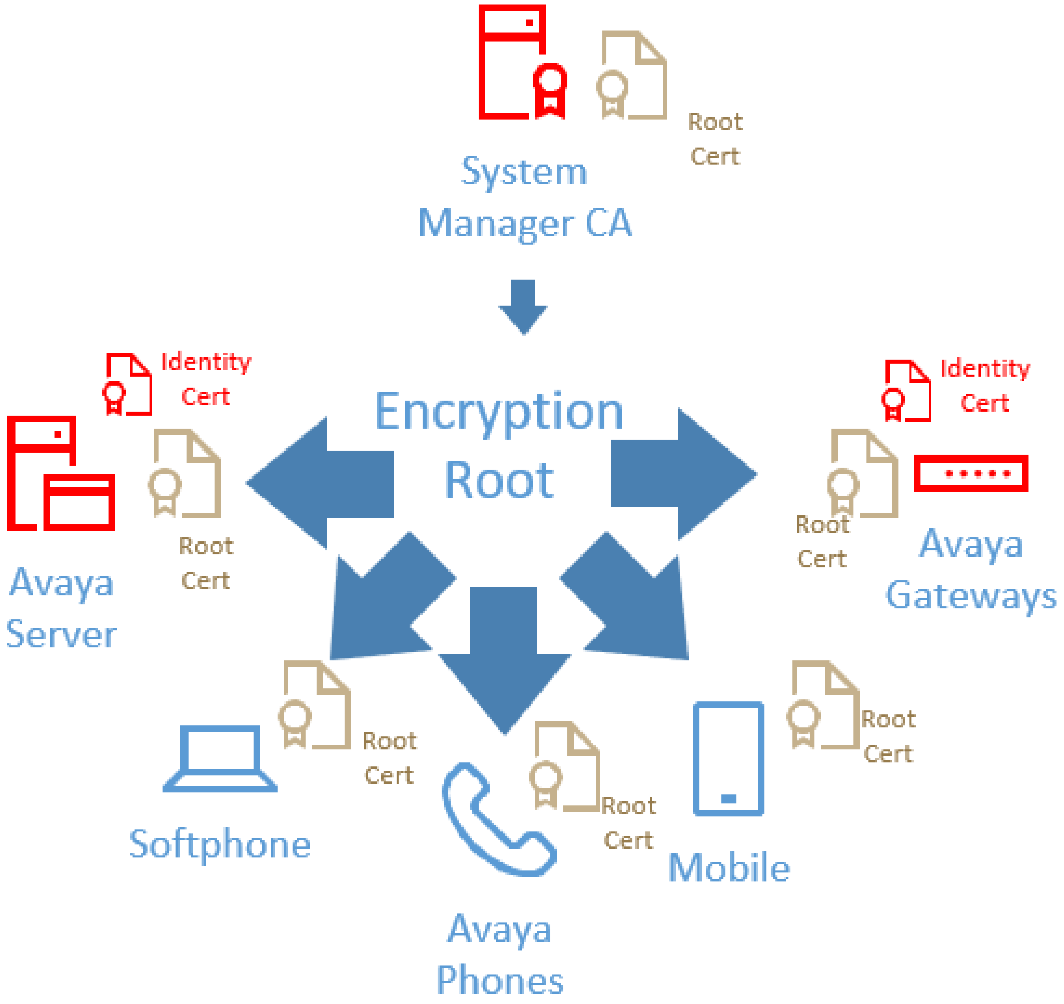
End entity certificate

End entity certificate

End entity certificate

End entity certificate

System Manager as the Certificate Authority



System Manager as the Certificate Authority

Pros

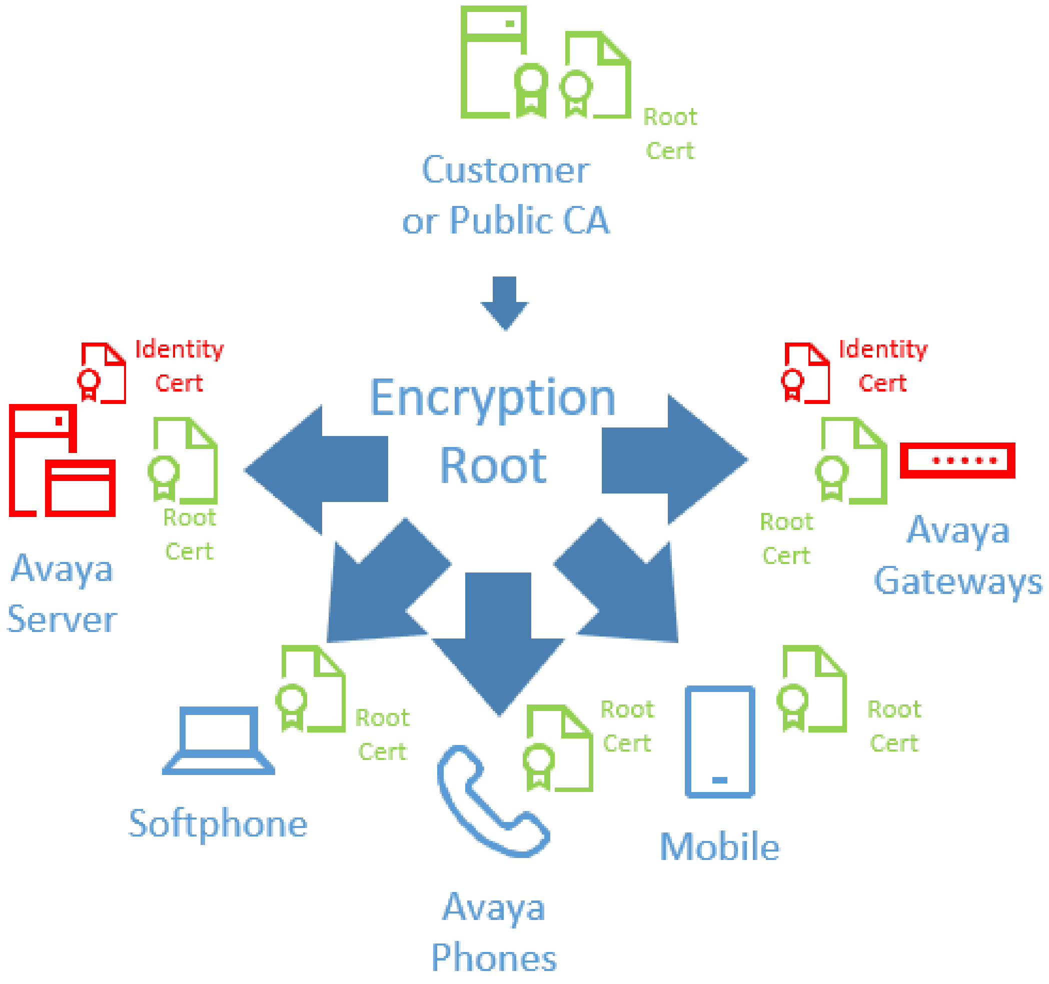
- Works out of box
- Automatically issues and deploys and redeploys certificates for managed elements (SMGR / SM) Aura environment stands alone
- Simplest - Easy to manage by customer & partners

Cons

- PKI is independent of other PKI
- No enterprise branding
- Must distribute PKI to endpoints

SECURITY

Enterprise Certificate Authority



Enterprise Certificate Authority

Pros

- Provide enterprise asserted trust
- Certificates may already be distributed to client devices.

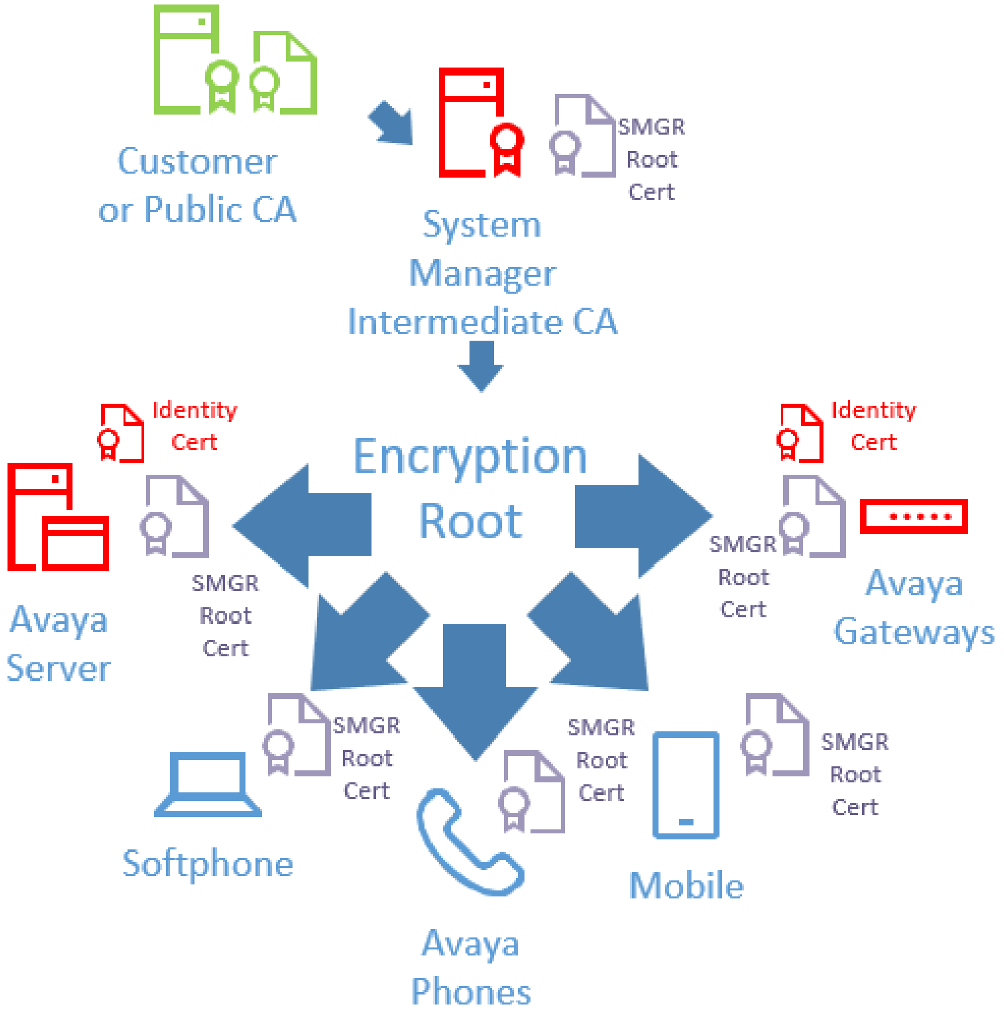
Cons

- Must manually establish PKI trust chain to Aura managed devices.
- Must create Certificate signing request and import identity certificates
- No automatic issue or re-issue of certificates.
- Involve IT for all certificates needed

Relatively straightforward deployment. Not require for all devices. (Can generate identity certs only for required)

SECURITY

System Manager as a Subordinate CA



System Manager as a Subordinate CA

Pros

- Provides enterprise certs.
- Certificates may already be distributed to client devices.
- Automatically issues and deploys and redeploys certificates for managed elements (SMGR / SM)

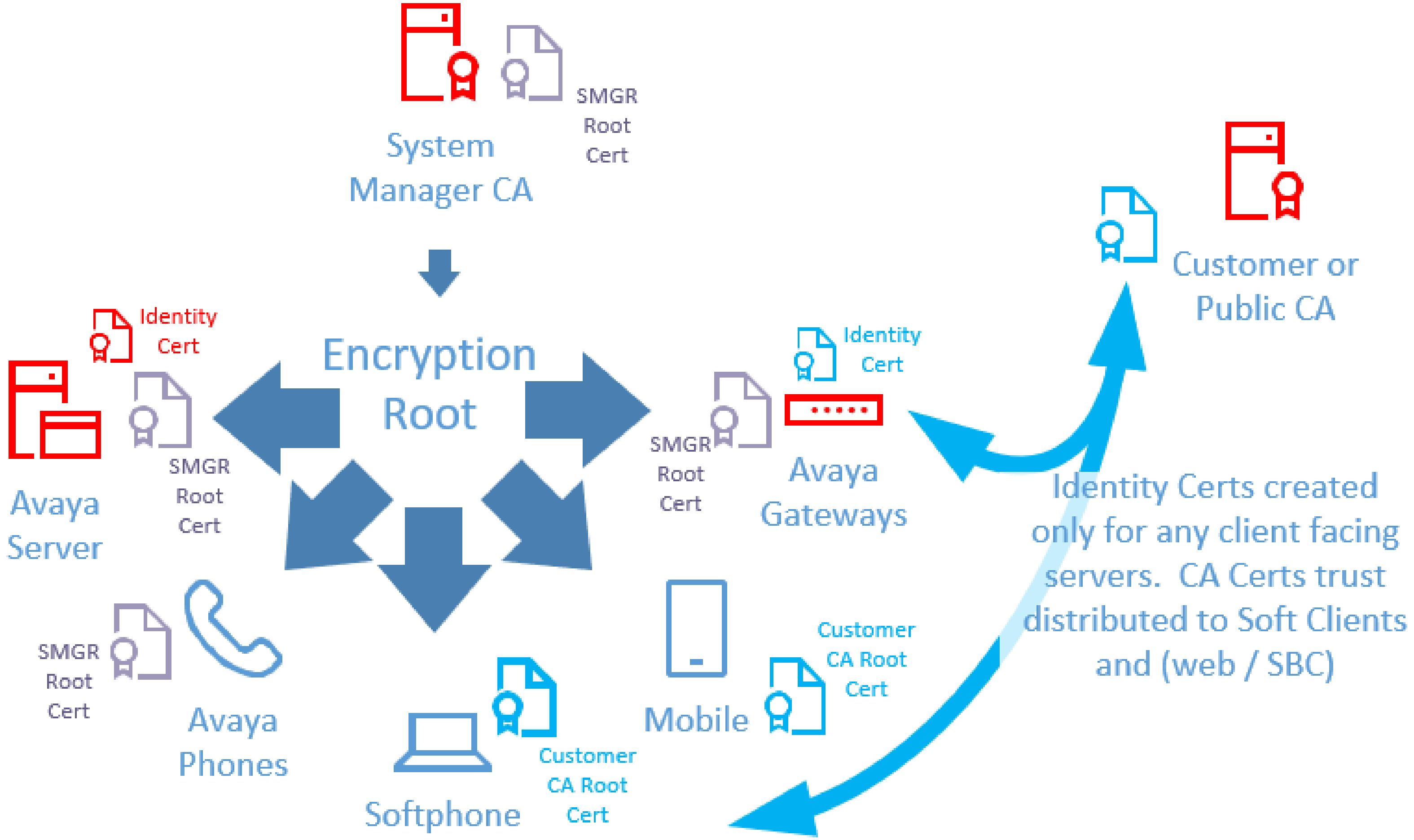
Cons

- Enterprise must allow sub-CA
- Trust chain must be distributed to all Aura elements

Difficult to implement but allows for a chain of trust to internal I/T. Usually not well received by I/T.

SECURITY

SMGR for Aura / Public CA where needed



Identity Certs created only for any client facing servers. CA Certs trust distributed to Soft Clients and (web / SBC)

SMGR for Aura / Public CA where needed

Pros

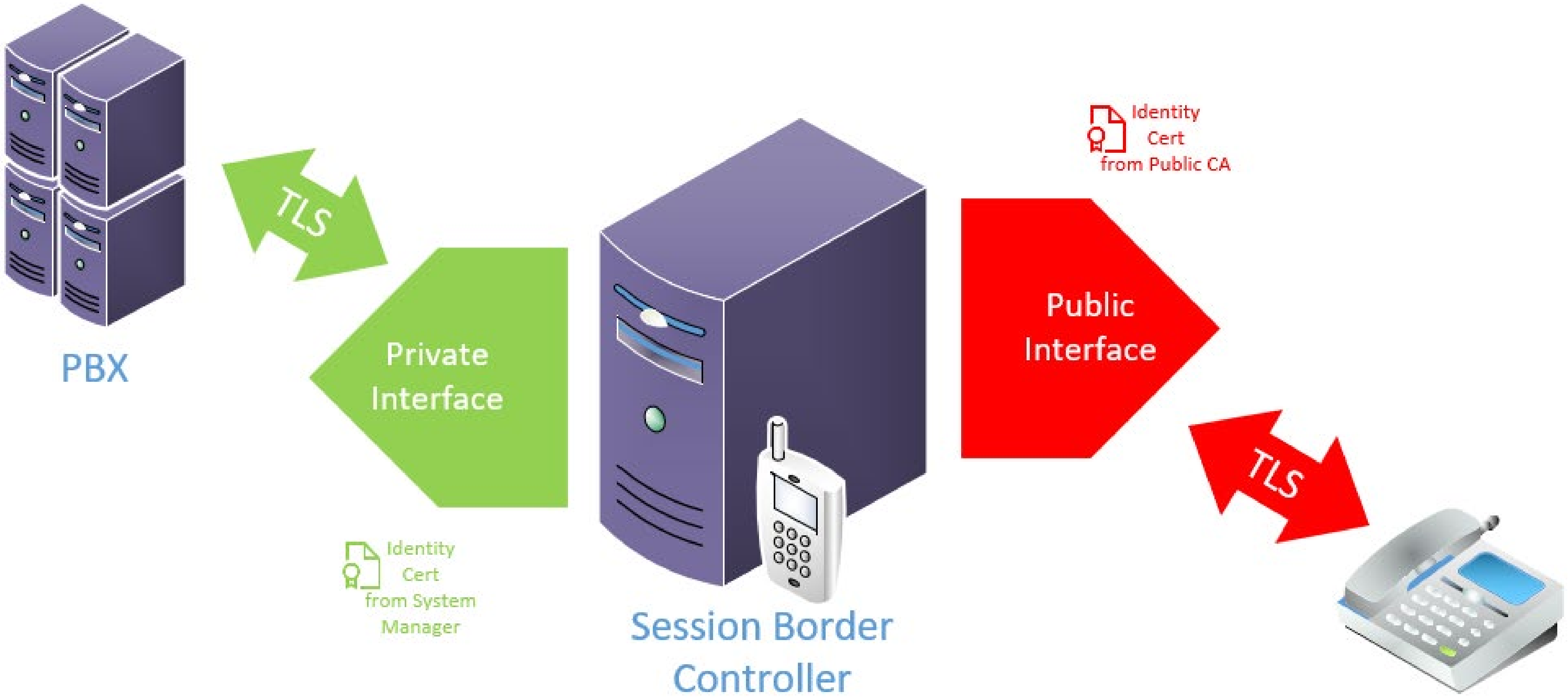
- Provides enterprise certs where needed.
- Allows SMGR to provide certs for Aura
- Certificates may already be distributed to client devices.
- Automatically issues and deploys and redeploys certificates for managed elements (SMGR / SM)
- Aura managed certs for most “internal” servers.

Cons

- Two PKI authorities

SECURITY

Examples of TLS links used by SBC – different certs signed by different CAs



TLS
PBX
Private Interface
Identity Cert from System Manager
Session Border Controller
Public Interface
Identity Cert from Public CA
TLS

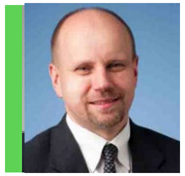
Questions / Comments / Applause / Boos…

What’s the best way for you to get help with security and certificates?

Find the best partner – here at the show!
Please fill out your session survey! Session 1088
Please tweet about the presentation if you liked it - @clauss

- Come ask us questions
- Call us – 888-777-7280
- Check us out online – www.convergeone.com
- Thanks for attending!

ConvergeOne



Chris Clauss
cclauss@convergeone.com