WHILE 1
SOFTWARE

PKI

A public key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository and revokes them if needed. (Wikipedia)

Why

To allow organizations to be independent in keys management with proper cyber security levels of protection and controlled costs in the years.

What

W1 PKI product and solution scale from low-end systems up to full cloud farms.

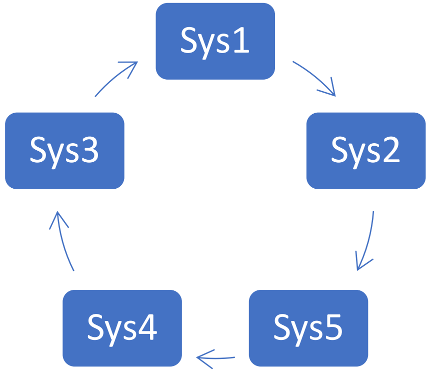
How

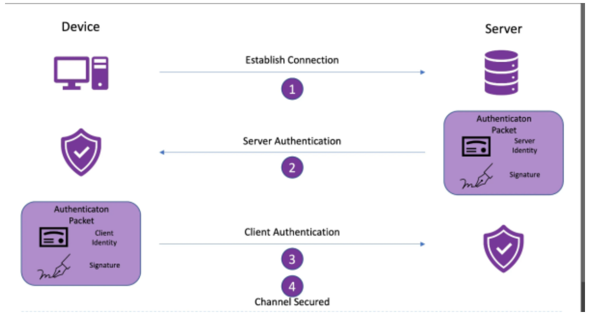
W1 PKI supports all flavors of deploy:

- In customer premises
- In customer cloud
- PAAS
- SAAS

while1.com // PKI >> Use Cases

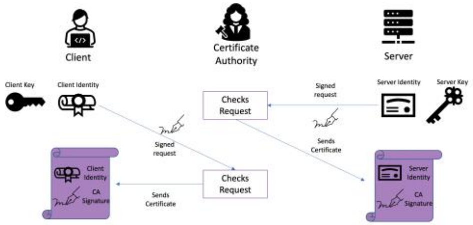
Protect communication among systems / implement zero trust approach



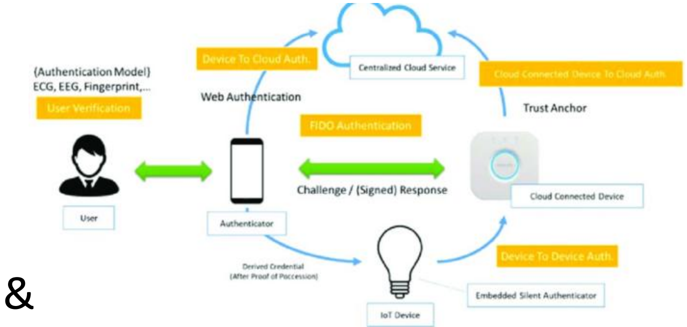


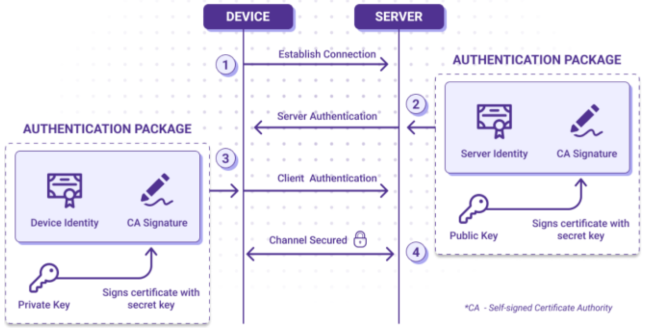
Ensure authenticity, integrity and confidentiality in client-server communications

Digital sign and validate data and documents.



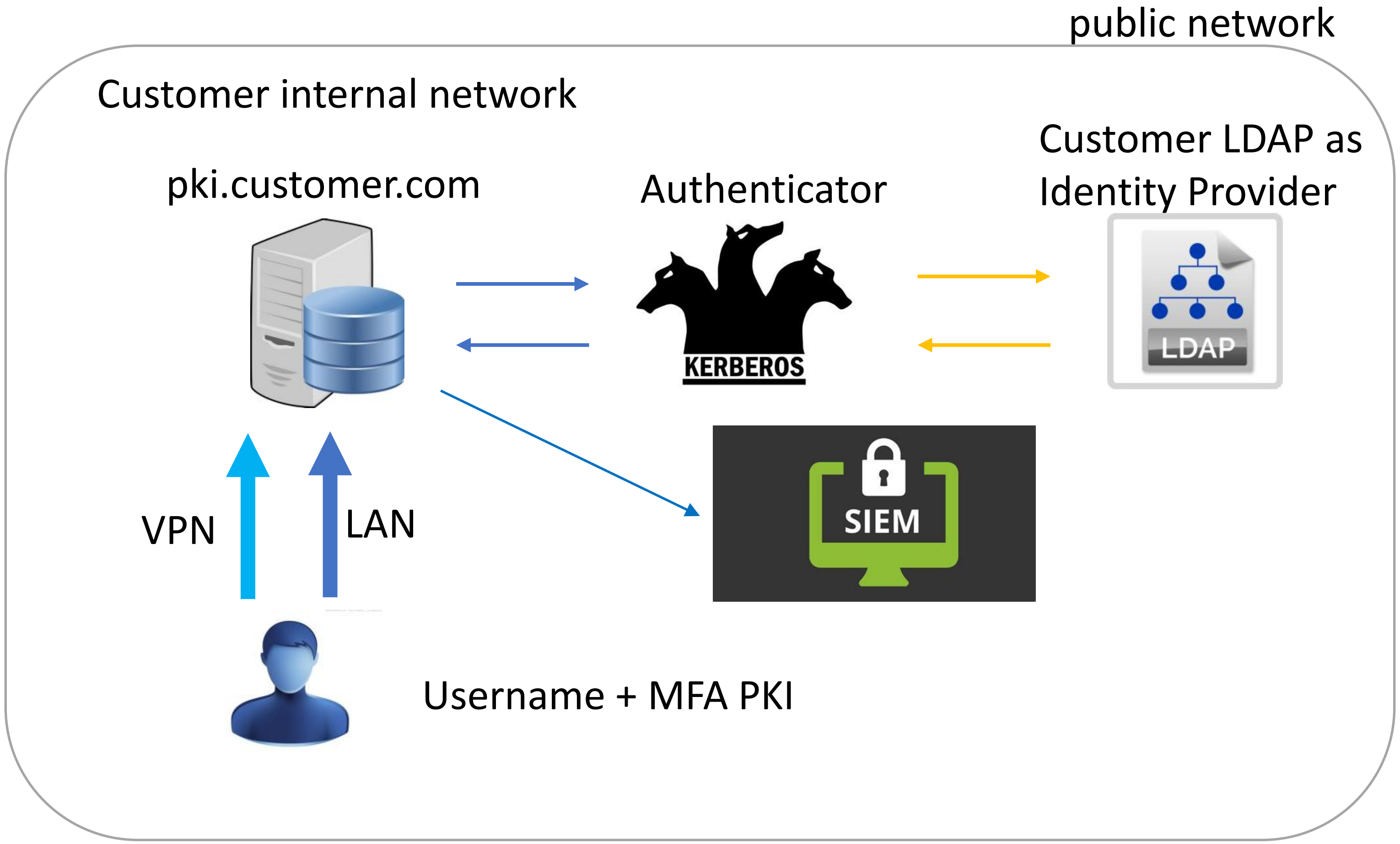
Enroll digital identities on mobile apps & devices, IoT devices





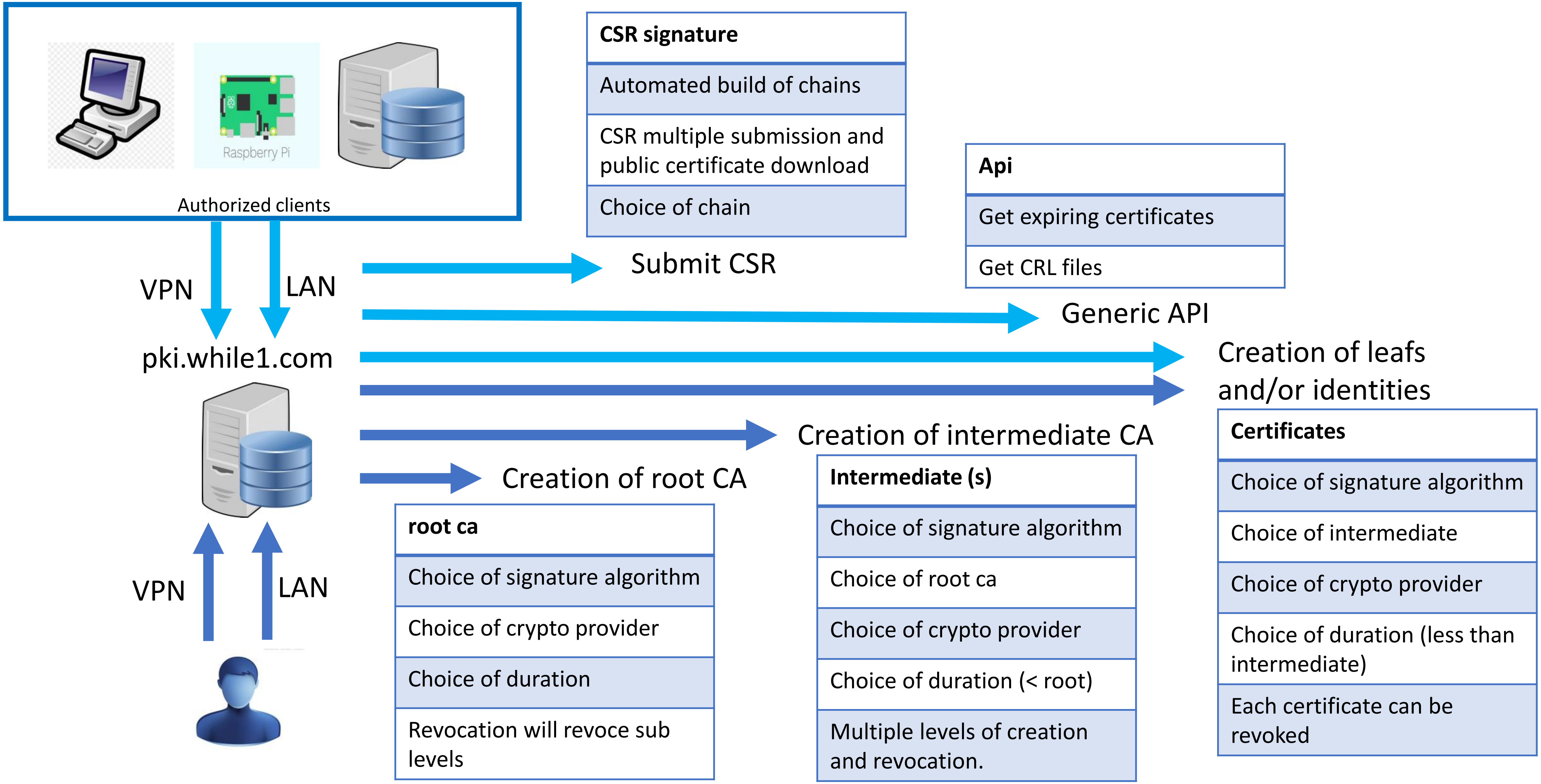
Implement repudiation and key-rolling automatic management and distribution

while1.com // PKI >> Macro schema, high level, on customer premise approach



HIGH LEVEL PROPERTIES
Integrated with customer identity and security provider
Reachibility according to customer design
Multiplatform capability
Siem feeder
Physical installation or contained installation as well

while1.com // PKI >> Macro schema, scenarios



Authorized clients

VPN

LAN

pki.while1.com

VPN

LAN

Submit CSR

Generic API

Creation of leafs and/or identities

Creation of intermediate CA

Creation of root CA

CSR signature
Automated build of chains
CSR multiple submission and public certificate download
Choice of chain

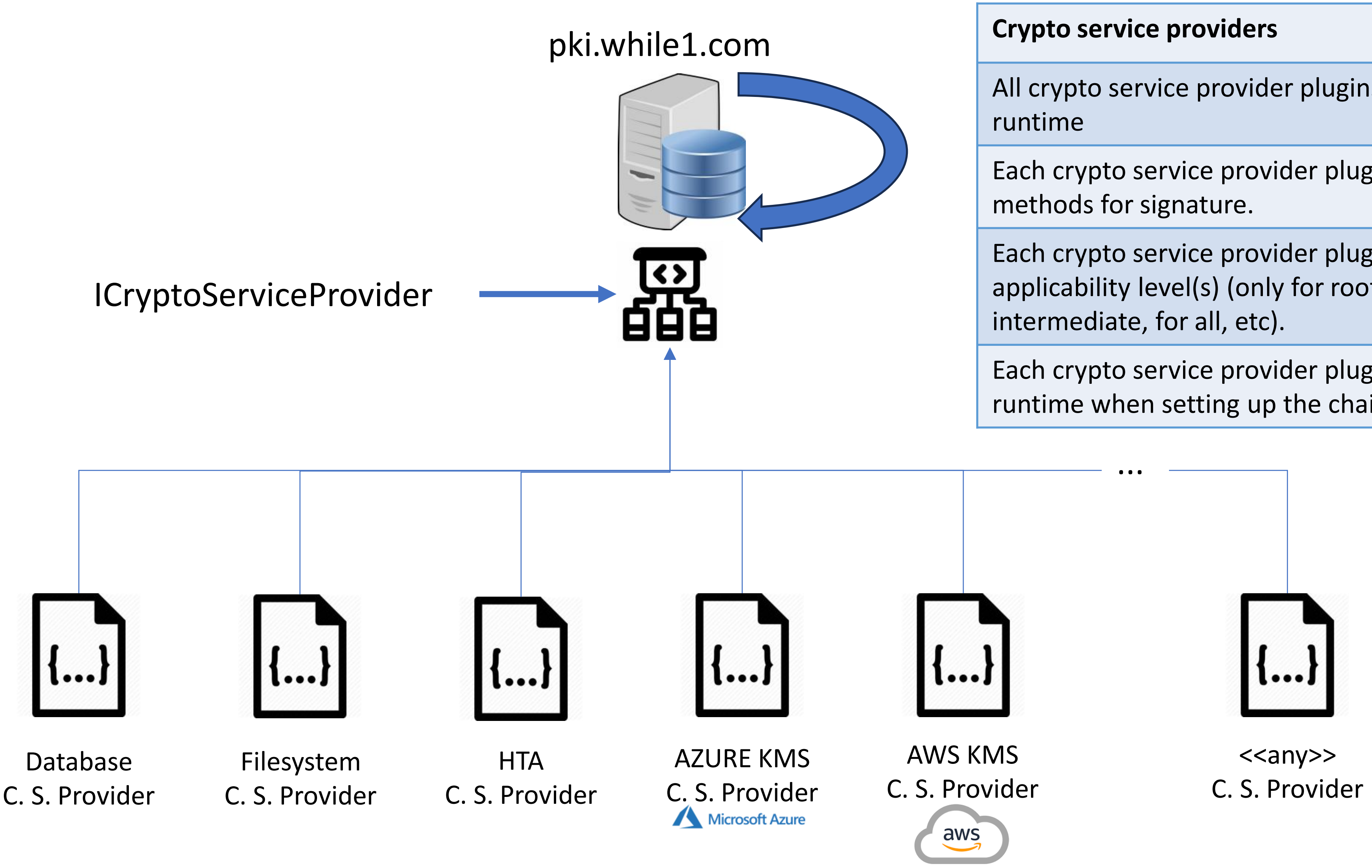
Api
Get expiring certificates
Get CRL files

root ca
Choice of signature algorithm
Choice of crypto provider
Choice of duration
Revocation will revoce sub levels

Intermediate (s)
Choice of signature algorithm
Choice of root ca
Choice of crypto provider
Choice of duration (< root)
Multiple levels of creation and revocation.

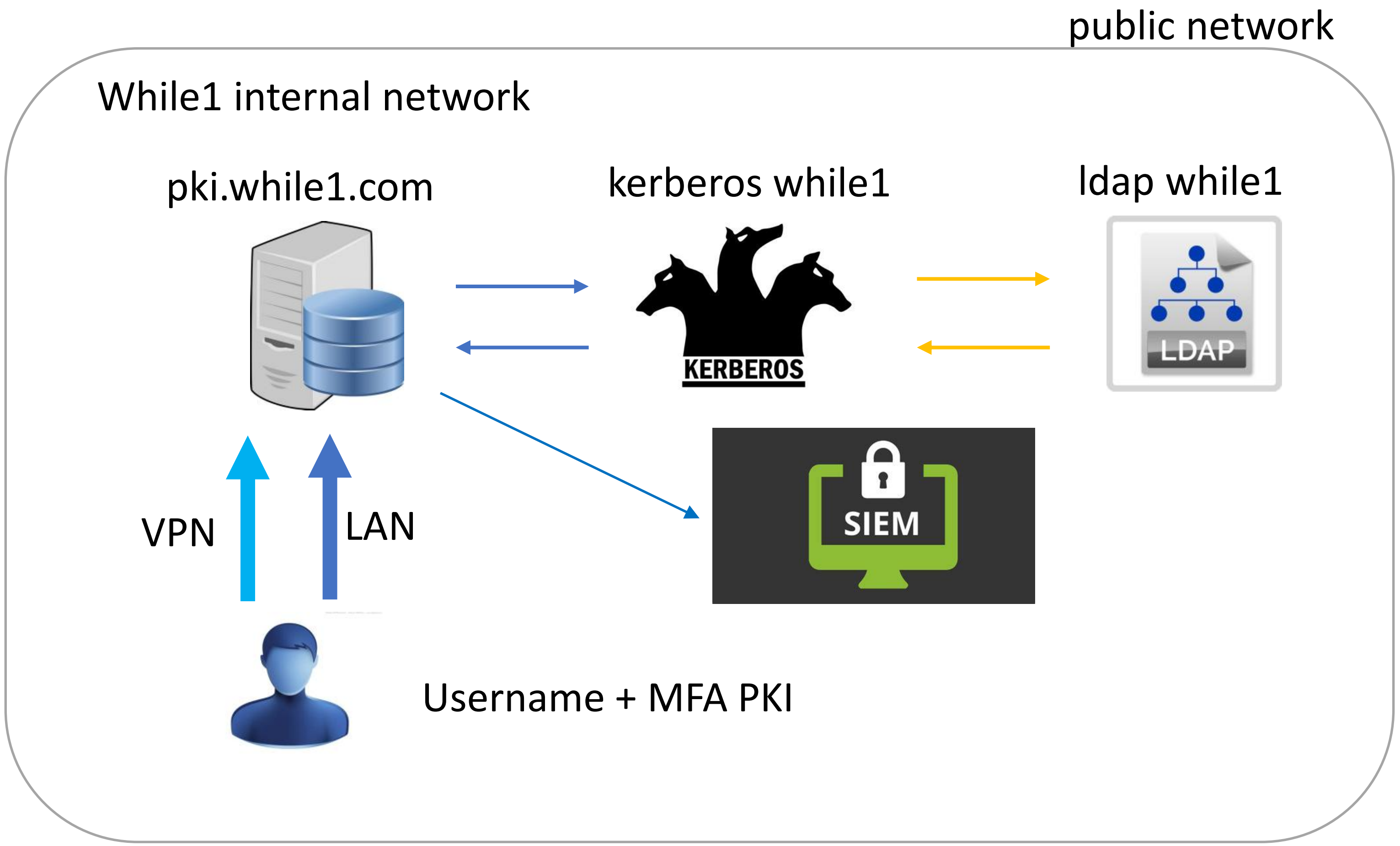
Certificates
Choice of signature algorithm
Choice of intermediate
Choice of crypto provider
Choice of duration (less than intermediate)
Each certificate can be revoked

while1.com // PKI >> CryptoServiceProvider concepts



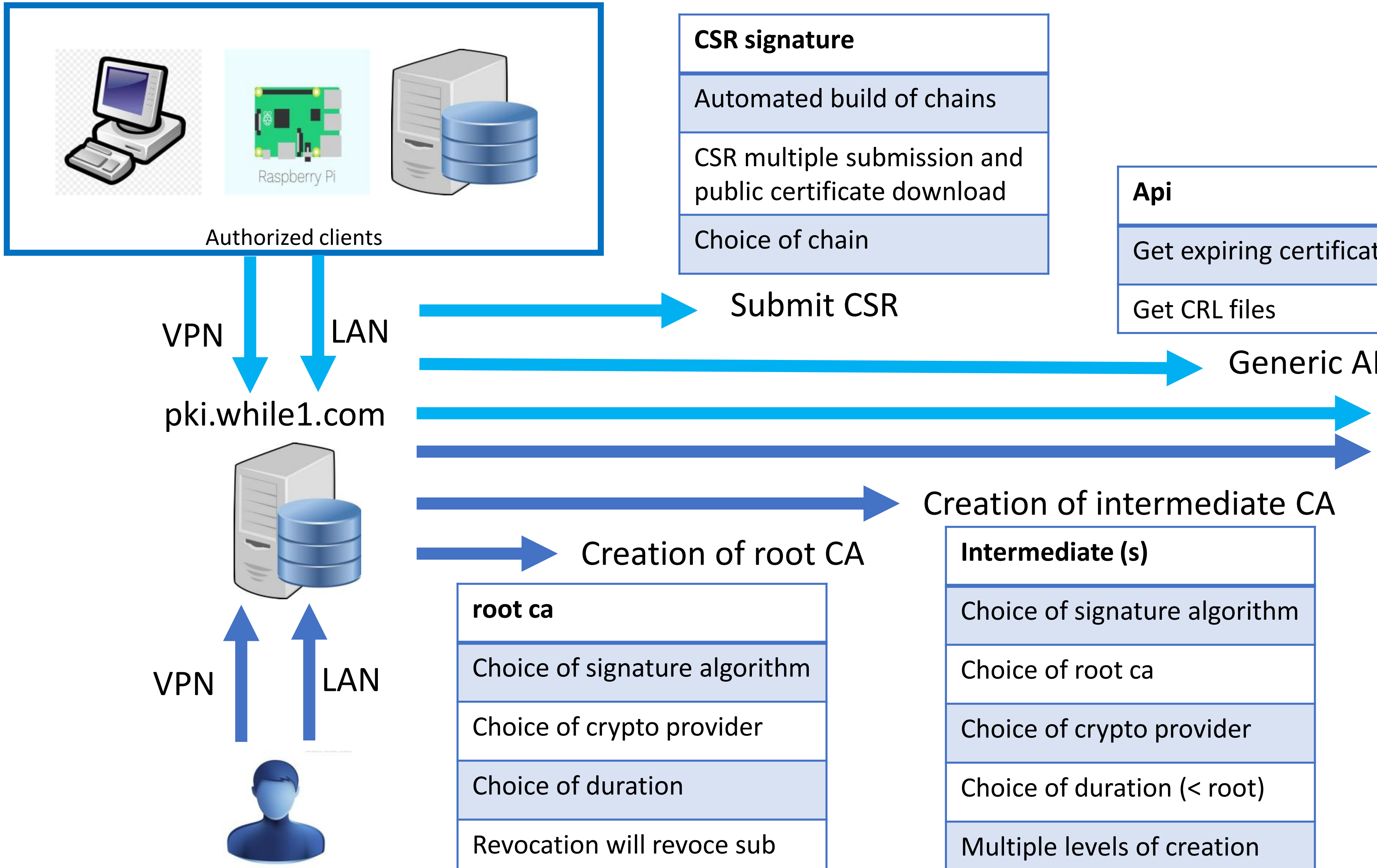
Crypto service providers
All crypto service provider plugins will be loaded runtime
Each crypto service provider plugin will define methods for signature.
Each crypto service provider plugin will define its applicability level(s) (only for root, for root and intermediate, for all, etc).
Each crypto service provider plugin will be usable at runtime when setting up the chain.

while1.com // PKI >> Macro schema, high level



HIGH LEVEL PROPERTIES
Integrated with internal security provider
Not exposed to internet
Multiplatform capability
Siem feeder
Physical installation or contained installation as well

while1.com // PKI >> Macro schema, real scenarios



Submit CSR

CSR signature
Automated build of chains
CSR multiple submission and public certificate download
Choice of chain

Generic API

Api
Get expiring certificates
Get CRL files

Creation of leafs and/or identities

Certificates
Choice of signature algorithm
Choice of intermediate
Choice of crypto provider
Choice of duration (less than intermediate)
Each certificate can be revoked

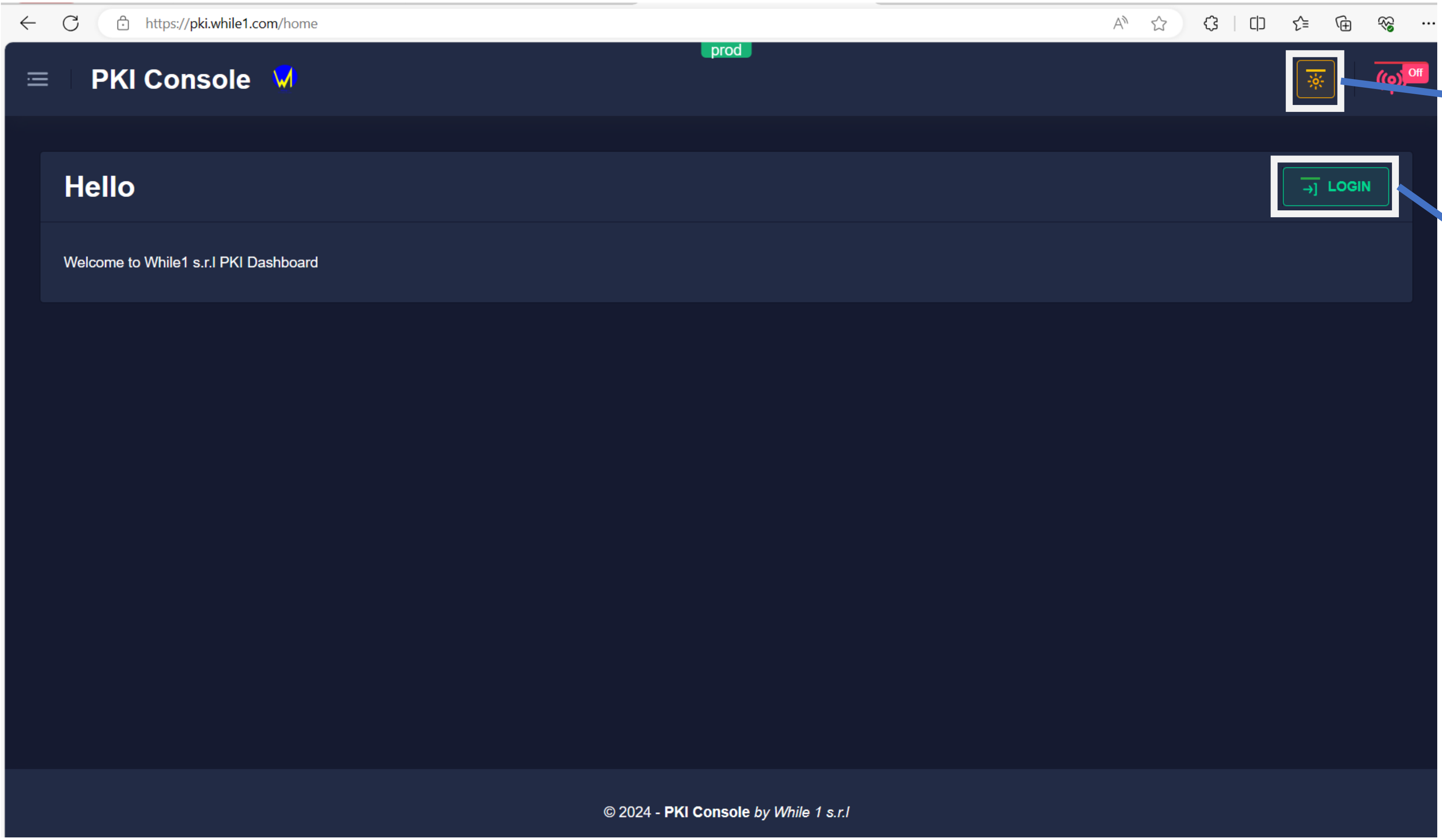
Creation of intermediate CA

Intermediate (s)
Choice of signature algorithm
Choice of root ca
Choice of crypto provider
Choice of duration (< root)
Multiple levels of creation and revocation.

Creation of root CA

root ca
Choice of signature algorithm
Choice of crypto provider
Choice of duration
Revocation will revoce sub levels

while1.com // PKI >> Welcome page



Hello

Welcome to While1 s.r.l PKI Dashboard

© 2024 - **PKI Console** *by While 1 s.r.l*

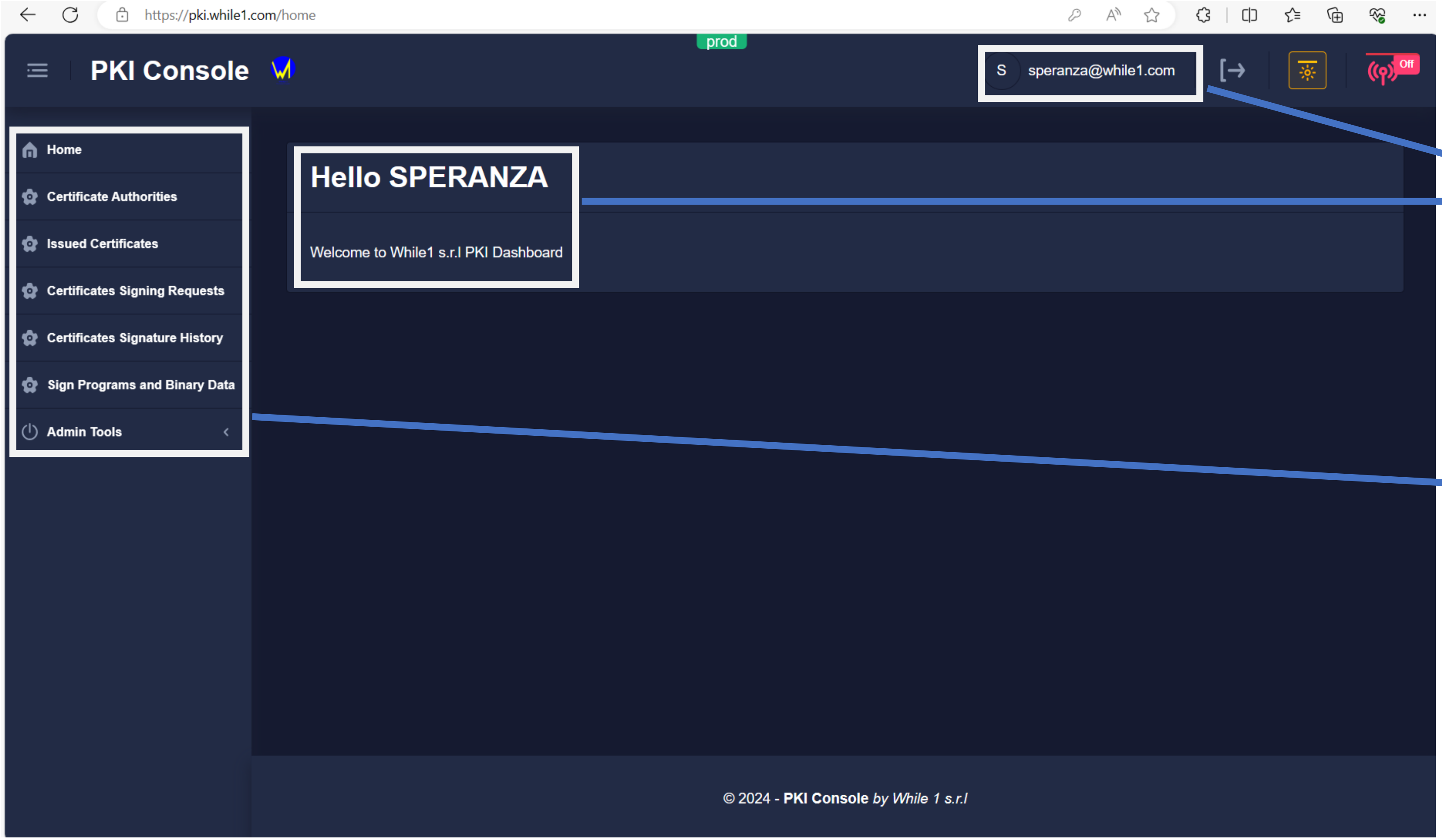
White or black layout

Proceed to login page.
Login providers supported are:

- ADFS
- LOCAL Provider
- Kerberos (over LDAP)

Other providers can be added with dedicated development

while1.com // PKI >> Activities



https://pki.while1.com/home
prod
PKI Console
S speranza@while1.com
Off
Home
Certificate Authorities
Issued Certificates
Certificates Signing Requests
Certificates Signature History
Sign Programs and Binary Data
Admin Tools

Hello SPERANZA

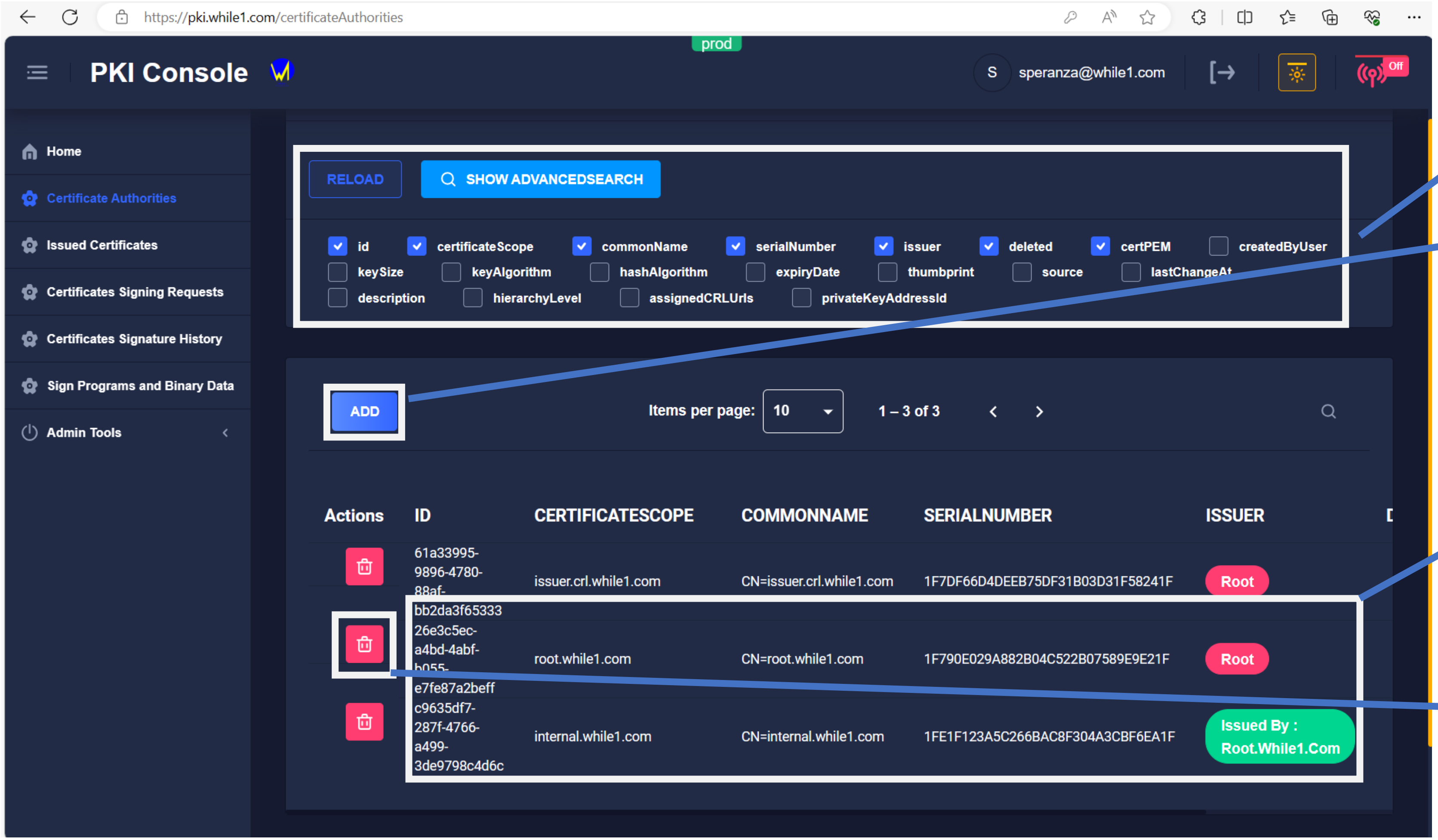
Welcome to While1 s.r.l PKI Dashboard

© 2024 - **PKI Console** *by While 1 s.r.l*

Reference to logged user

List of actions that user can perform. Authorization for user is bases on functionality

while1.com // PKI >> root and intermediates


https://pki.while1.com/certificateAuthorities
prod
PKI Console
S
speranza@while1.com
Off
Home
Certificate Authorities
Issued Certificates
Certificates Signing Requests
Certificates Signature History
Sign Programs and Binary Data
Admin Tools
RELOAD
SHOW ADVANCEDSEARCH
ADD

☑ id ☑ certificateScope ☑ commonName ☑ serialNumber ☑ issuer ☑ deleted ☑ certPEM □ createdByUser
□ keySize □ keyAlgorithm □ hashAlgorithm □ expiryDate □ thumbprint □ source □ lastChangeAt
□ description □ hierarchyLevel □ assignedCRLUrls □ privateKeyAddressId

Items per page: 10 1 – 3 of 3

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
🗑	61a33995- 9896-4780- 88af- bb2da3f65333	issuer.crl.while1.com	CN=issuer.crl.while1.com	1F7DF66D4DEEB75DF31B03D31F58241F	Root
🗑	26e3c5ec- a4bd-4abf- b055- e7fe87a2beff	root.while1.com	CN=root.while1.com	1F790E029A882B04C522B07589E9E21F	Root
🗑	c9635df7- 287f-4766- a499- 3de9798c4d6c	internal.while1.com	CN=internal.while1.com	1FE1F123A5C266BAC8F304A3CBF6EA1F	Issued By : Root.While1.Com

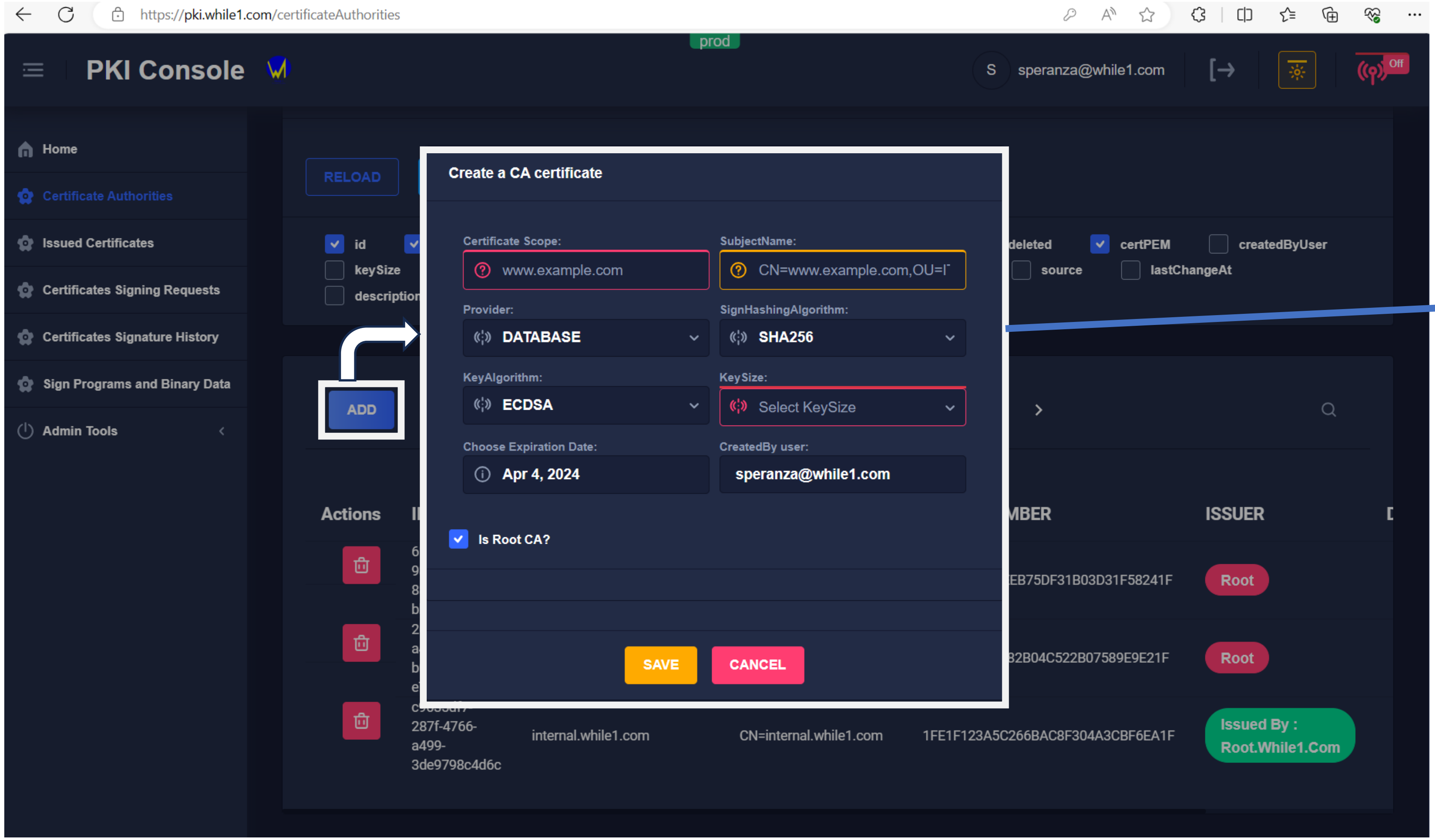
Filter for search. All fields are filterable and produce immediate result

Button to add root or intermediate. Explain in the next slide

Minimum details for each issued root or intermediate certificate. If the certificate is a root certificate, the issuer will itself, otherwise the name of the issuer (for example an intermediate)

The delete button will delete the certificate. If level has sub levels, you can delete all signed certificate. The delete will automatically populate the CRL file.

while1.com // PKI >> Add new certificate



Create a CA certificate

Certificate Scope: www.example.com

SubjectName: CN=www.example.com,OU=I

Provider: DATABASE

SignHashingAlgorithm: SHA256

KeyAlgorithm: ECDSA

KeySize: Select KeySize

Choose Expiration Date: Apr 4, 2024

CreatedBy user: speranza@while1.com

☑ Is Root CA?

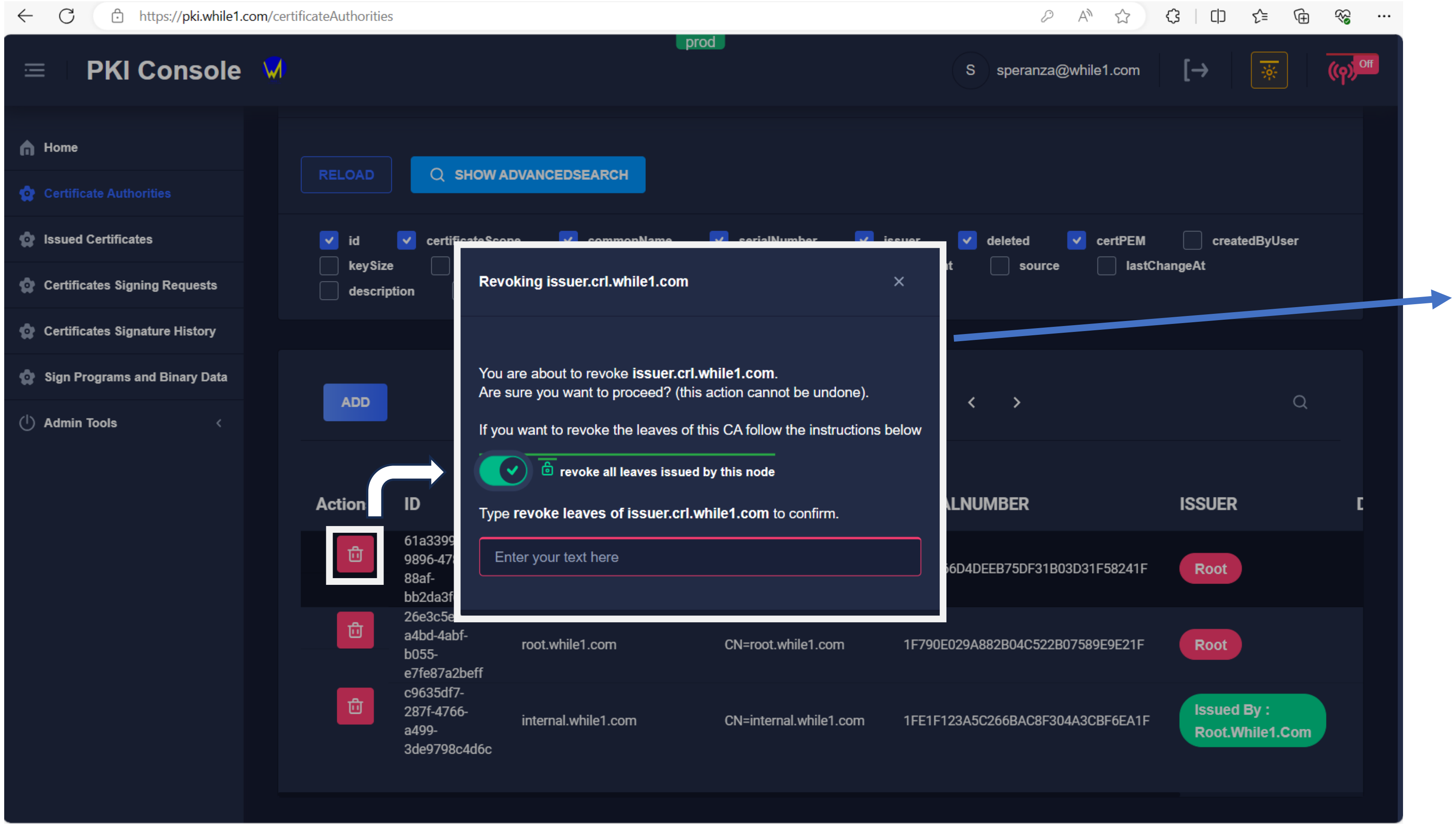
SAVE CANCEL

In this dialog we add a root certificate or a intermediate certificate. Properties are:

- Certificate scope → a label (root.while1.com)
- Subject name → if empty, automatically built, else it can be fully specified
- Provider → a list of possible signature provider*
- SignHashingAlgorithm, KeyAlgorith, Keysize → possible combination of valid values and size
- Choose Expiration Date → you can choose the expiration date that best fit the needs.
- Is Root CA → if selected, the certificate is a root certificate, if not selected, the certificate is intermediate and a root can be selected.

* Providers can be developped to fit a need. An interface is shared. The implementation of that interface will allow to have a new available provider

while1.com // PKI >> delete a certificate


https://pki.while1.com/certificateAuthorities
prod
PKI Console
S speranza@while1.com
Off
Home
Certificate Authorities
Issued Certificates
Certificates Signing Requests
Certificates Signature History
Sign Programs and Binary Data
Admin Tools
RELOAD
SHOW ADVANCEDSEARCH
ADD

☑ id ☑ certificateScope ☑ commonName ☑ serialNumber ☑ issuer ☑ deleted ☑ certPEM □ createdByUser
□ keySize □ source □ lastChangeAt
□ description

Revoking issuer.crl.while1.com ×

You are about to revoke **issuer.crl.while1.com**.
Are sure you want to proceed? (this action cannot be undone).

If you want to revoke the leaves of this CA follow the instructions below

☑ **revoke all leaves issued by this node**

Type **revoke leaves of issuer.crl.while1.com** to confirm.

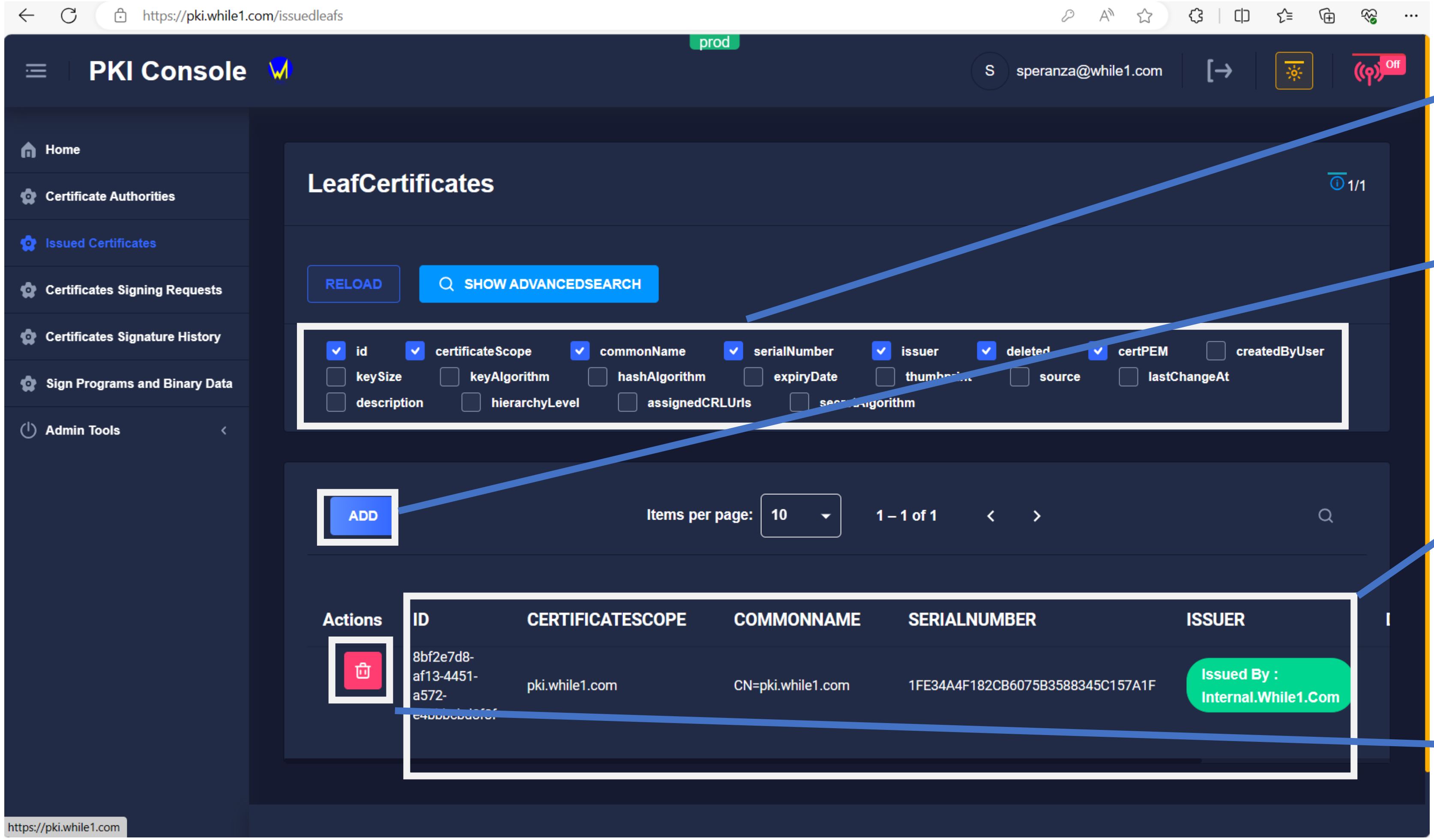
Enter your text here

Action	ID			LNUMBER	ISSUER	D
	61a3399 9896-47 88af- bb2da3f			6D4DEEB75DF31B03D31F58241F	Root	
	26e3c5e a4bd-4abf- b055- e7fe87a2beff	root.while1.com	CN=root.while1.com	1F790E029A882B04C522B07589E9E21F	Root	
	c9635df7- 287f-4766- a499- 3de9798c4d6c	internal.while1.com	CN=internal.while1.com	1FE1F123A5C266BAC8F304A3CBF6EA1F	Issued By : Root.While1.Com	

The deletion of a certificate requires a strong confirmation because:

- All signed certificates will be deleted
- All deleted certificates will be added to CRL file

while1.com // PKI >> manage leaf certificates



https://pki.while1.com/issuedleafs

prod

PKI Console

S speranza@while1.com

Off

- Home
- Certificate Authorities
- Issued Certificates
- Certificates Signing Requests
- Certificates Signature History
- Sign Programs and Binary Data
- Admin Tools

LeafCertificates

1/1

RELOAD

SHOW ADVANCEDSEARCH

☑ id ☑ certificateScope ☑ commonName ☑ serialNumber ☑ issuer ☑ deleted ☑ certPEM □ createdByUser
□ keySize □ keyAlgorithm □ hashAlgorithm □ expiryDate □ thumbprint □ source □ lastChangeAt
□ description □ hierarchyLevel □ assignedCRLUrls □ secretAlgorithm

ADD

Items per page: 10

1 – 1 of 1

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
🗑	8bf2e7d8-af13-4451-a572-[illegible]	pki.while1.com	CN=pki.while1.com	1FE34A4F182CB6075B3588345C157A1F	Issued By : Internal.While1.Com

https://pki.while1.com

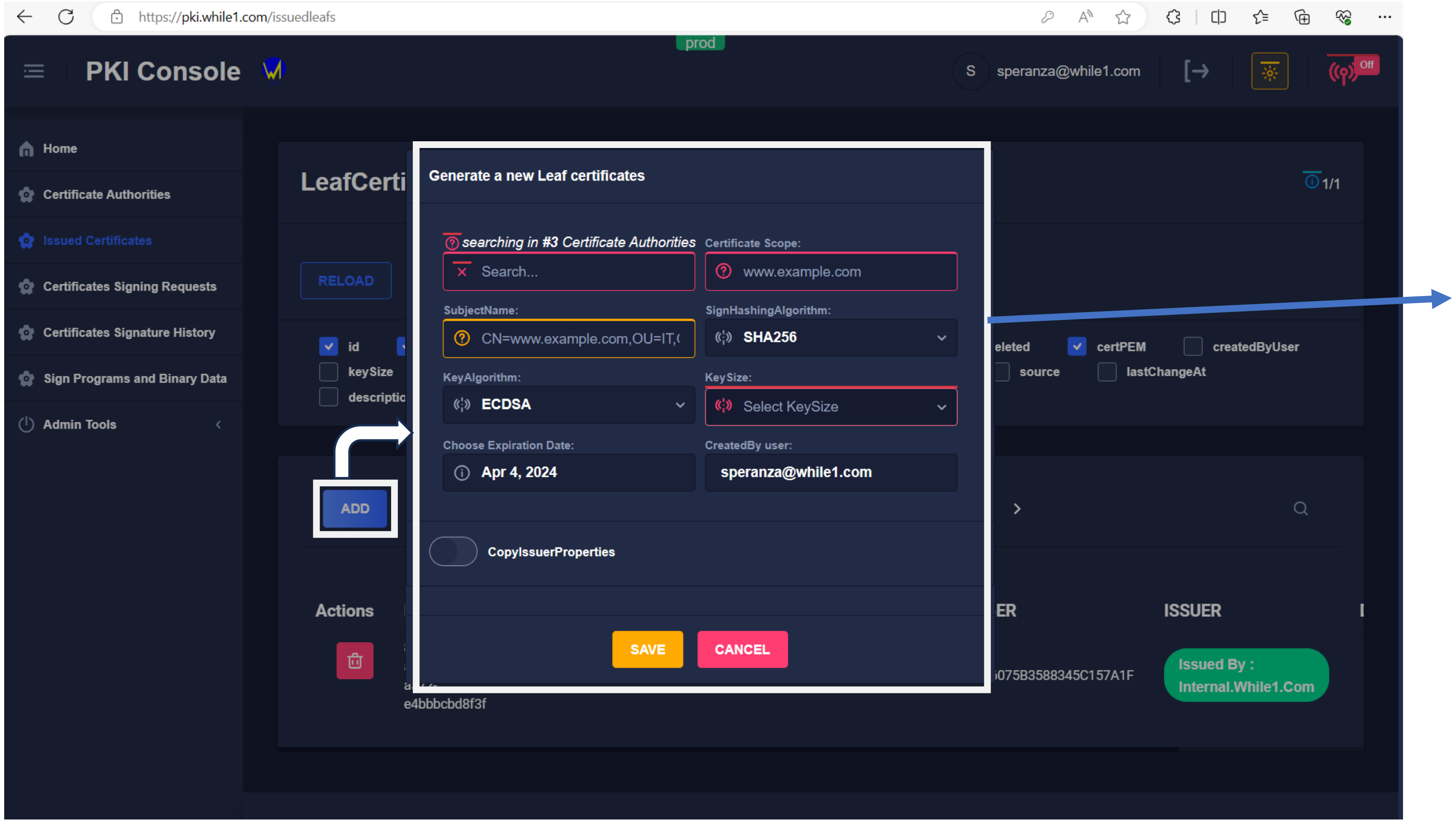
Filter for search. All fields are filterable and produce immediate result

Button to add a leaf certificate. Explain in the next slide

Minimum details for each leaf certificate. The issuer is a intermediate or a root certificate, previously managed.

The delete button will delete the certificate. Since the certificate is a leaf, the deletion will impact and add to CRL this certificate only.

while1.com // PKI >> add new leaf certificate



Generate a new Leaf certificates

searching in #3 Certificate Authorities: Search...

Certificate Scope: www.example.com

SubjectName: CN=www.example.com,OU=IT,(

SignHashingAlgorithm: SHA256

KeyAlgorithm: ECDSA

KeySize: Select KeySize

Choose Expiration Date: Apr 4, 2024

CreatedBy user: speranza@while1.com

○ CopyIssuerProperties

☑ id ☐ keySize ☐ descriptio

eleted ☐ source ☑ certPEM ☐ lastChangeAt ☐ createdByUser

a e4bbbcbd8f3f

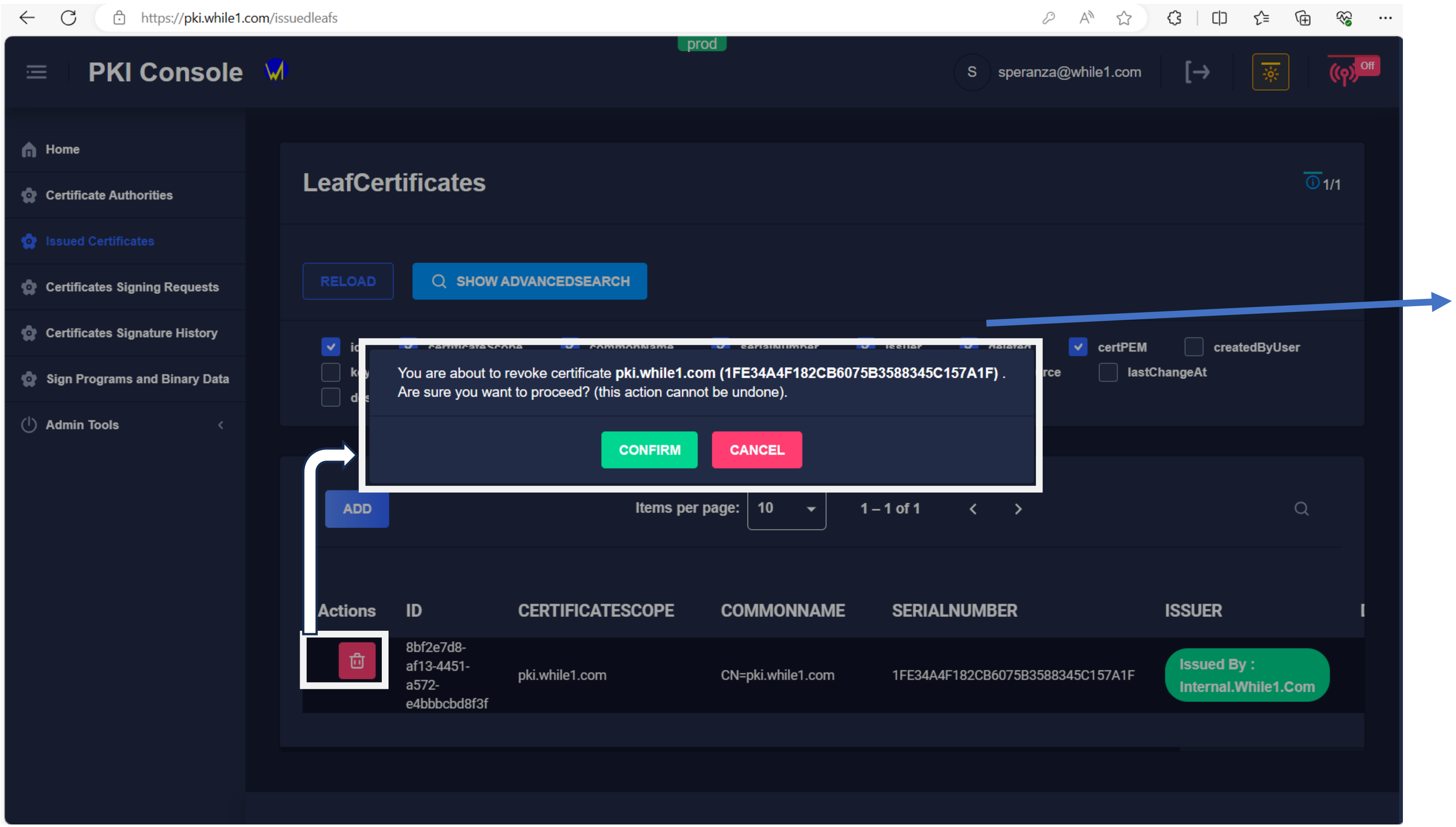
075B3588345C157A1F

Issued By : Internal.While1.Com

In this dialog we new leaf certificate. Properties are:

- The certificate authorities → the root or intermediate certificate selected as signer
- Certificate scope → a label (myleaf.while1.com)
- Subject name → if empty, automatically built, else it can be fully specified
- SignHashingAlgorithm, KeyAlgorith, Keysize → possible combination of valid values and size
- Choose Expiration Date → you can choose the expiration date that best fit the needs. It cannot exceed the signer expiration date.
- Copy Issuer Properties → selecting this feature, all cryptography attributes will be inherited from the signer.

while1.com // PKI >> delete a leaf certificate



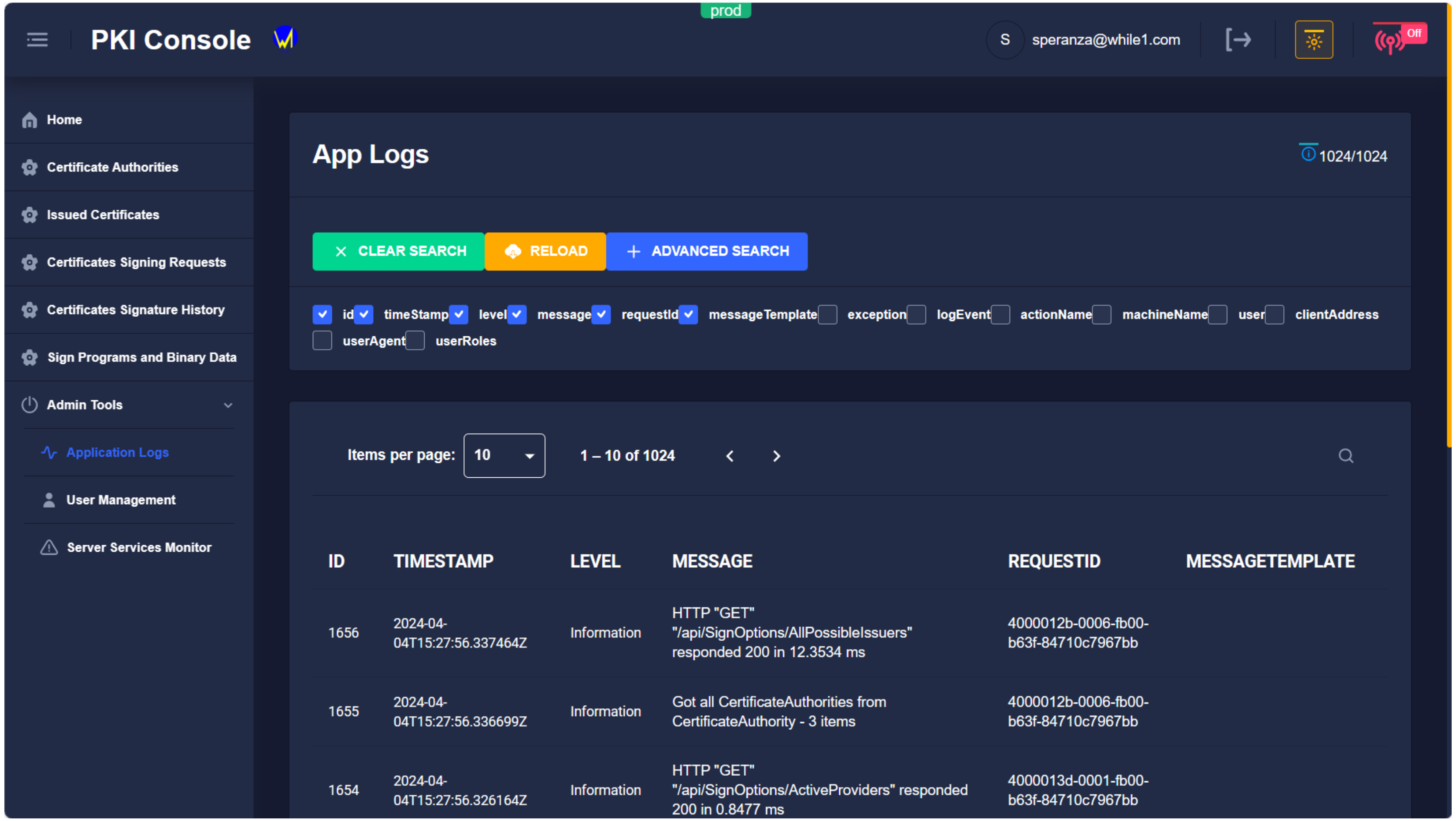
You are about to revoke certificate **pki.while1.com (1FE34A4F182CB6075B3588345C157A1F)** .
Are sure you want to proceed? (this action cannot be undone).

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
	8bf2e7d8-af13-4451-a572-e4bbbcbd8f3f	pki.while1.com	CN=pki.while1.com	1FE34A4F182CB6075B3588345C157A1F	Issued By : Internal.While1.Com

In this dialog we can delete a leaf certificate.
The deletion will affect only this certificate. The serial number of the certificate will be automatically inserted in crl file.

A new certificate with same common name can be created again.

while1.com // PKI >> application logs



App Logs

1024/1024

☑ id ☑ timeStamp ☑ level ☑ message ☑ requestId ☑ messageTemplate □ exception □ logEvent □ actionName □ machineName □ user □ clientAddress
□ userAgent □ userRoles

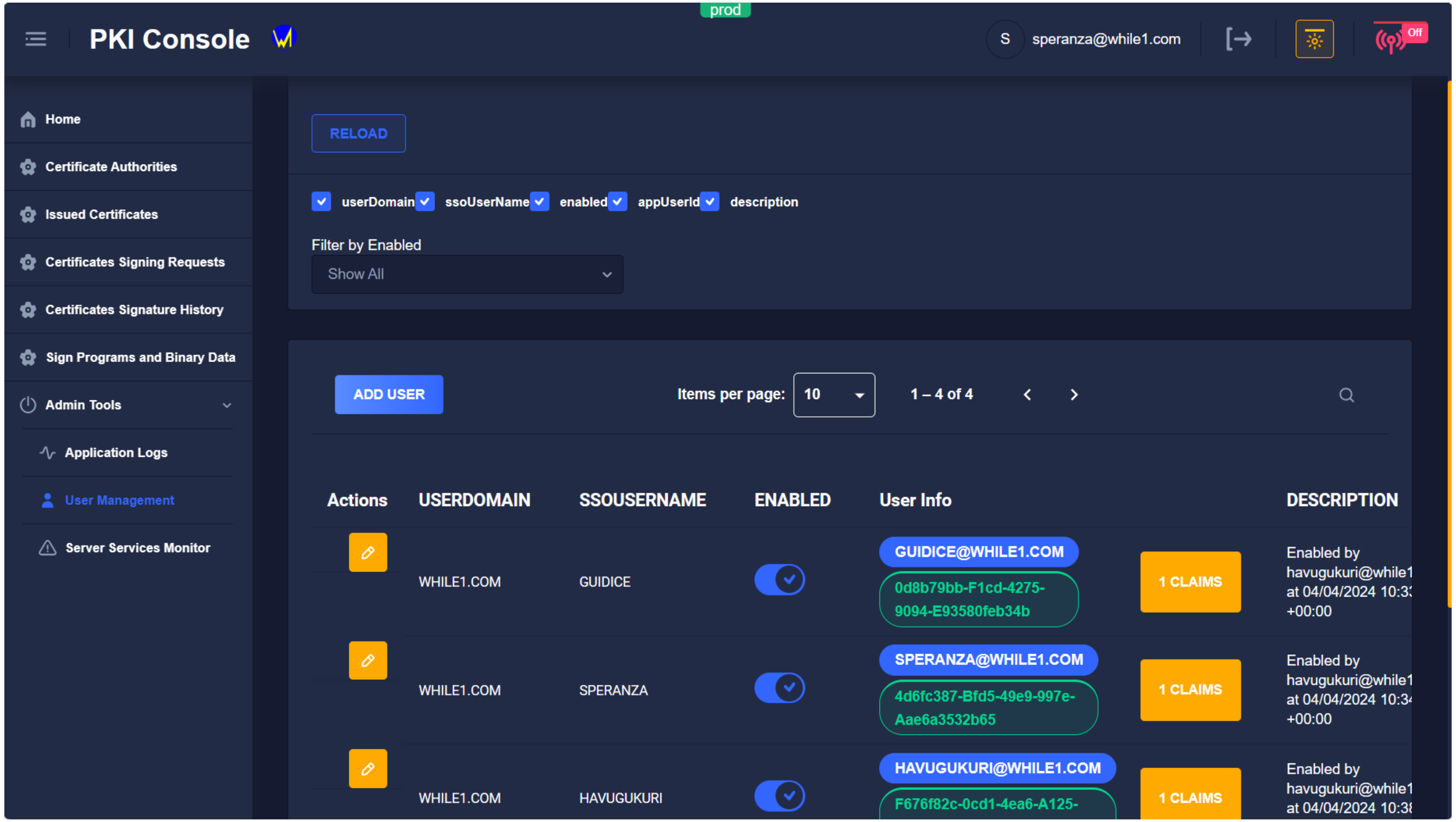
Items per page: 10   1 – 10 of 1024

ID	TIMESTAMP	LEVEL	MESSAGE	REQUESTID	MESSAGETEMPLATE
1656	2024-04-04T15:27:56.337464Z	Information	HTTP "GET" "/api/SignOptions/AllPossibleIssuers" responded 200 in 12.3534 ms	4000012b-0006-fb00-b63f-84710c7967bb	
1655	2024-04-04T15:27:56.336699Z	Information	Got all CertificateAuthorities from CertificateAuthority - 3 items	4000012b-0006-fb00-b63f-84710c7967bb	
1654	2024-04-04T15:27:56.326164Z	Information	HTTP "GET" "/api/SignOptions/ActiveProviders" responded 200 in 0.8477 ms	4000013d-0001-fb00-b63f-84710c7967bb	

In this page, an authorized user can search into logs.

This page in meant for administrative purposes only.

while1.com // PKI >> user management



☑ userDomain ☑ ssoUserName ☑ enabled ☑ appUserId ☑ description

Filter by Enabled: Show All

Items per page: 10 1 – 4 of 4

Actions	USERDOMAIN	SSOUSERNAME	ENABLED	User Info		DESCRIPTION
✎	WHILE1.COM	GUIDICE	✓	GUIDICE@WHILE1.COM 0d8b79bb-F1cd-4275-9094-E93580feb34b	1 CLAIMS	Enabled by havugukuri@while1 at 04/04/2024 10:3: +00:00
✎	WHILE1.COM	SPERANZA	✓	SPERANZA@WHILE1.COM 4d6fc387-Bfd5-49e9-997e-Aae6a3532b65	1 CLAIMS	Enabled by havugukuri@while1 at 04/04/2024 10:3 +00:00
✎	WHILE1.COM	HAVUGUKURI	✓	HAVUGUKURI@WHILE1.COM F676f82c-0cd1-4ea6-A125-	1 CLAIMS	Enabled by havugukuri@while1 at 04/04/2024 10:3

In this page, an authorized user can add or revoke a user.

This page in meant for administrative purposes only.

Hidden api	Scope
submitCSR	This api allows an authorized client to push a CSR and get back a signed certificate. This api allow to specify the provider to be used.
expiringCertificates	This api allows an authorized client to ask for list of certificate that are going to expire in {xx} days.