



**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

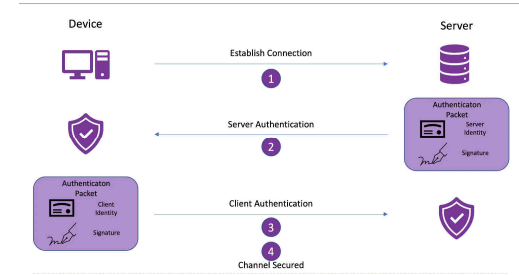
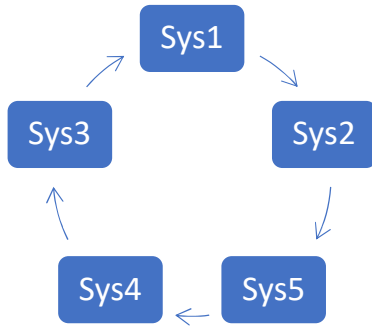
W1 PKI supports all flavors of deploy:

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



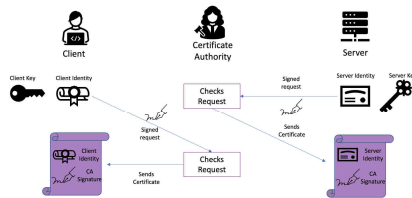
while1.com // PKI >> Use Cases

Protect communication among systems / implement zero trust approach

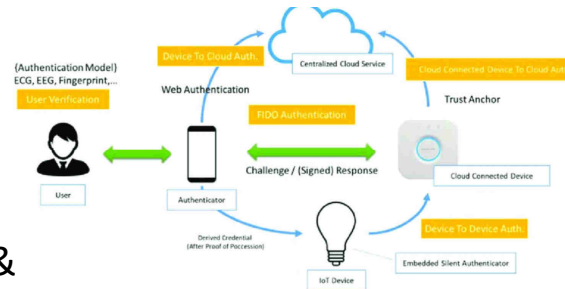


Ensure authenticity, integrity and confidentiality in client-server communications

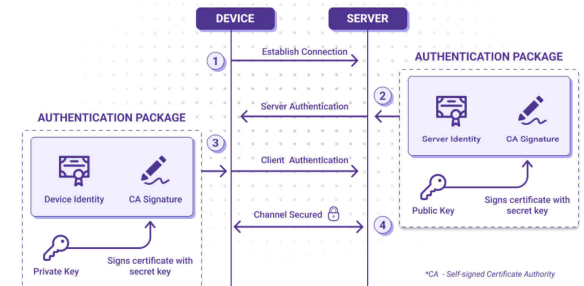
Digital sign and validate data and documents.



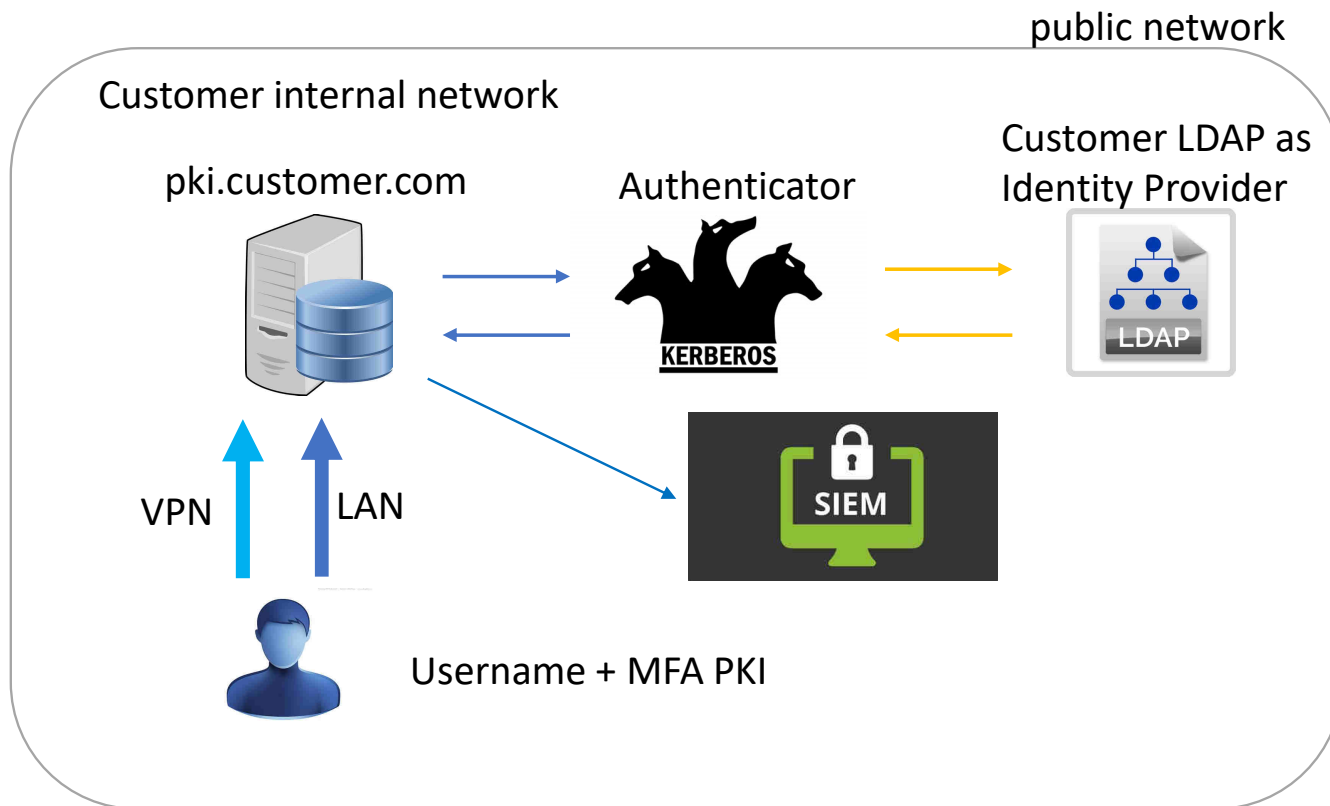
Enroll digital identities on mobile apps & devices, IoT devices



While 1 - Confidential



Implement repudiation and key-rolling automatic management and distribution



### HIGH LEVEL PROPERTIES

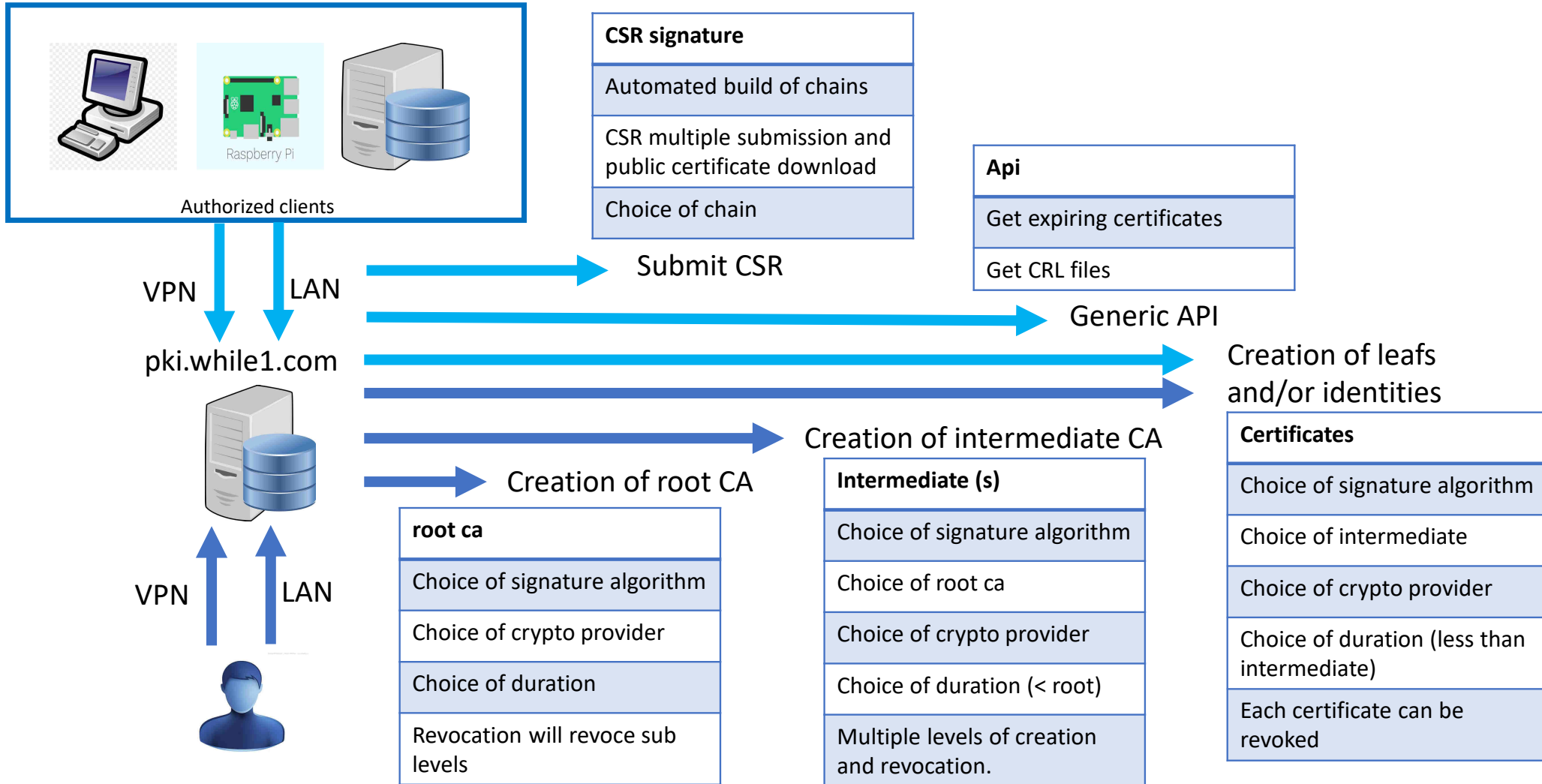
Integrated with customer identity and security provider

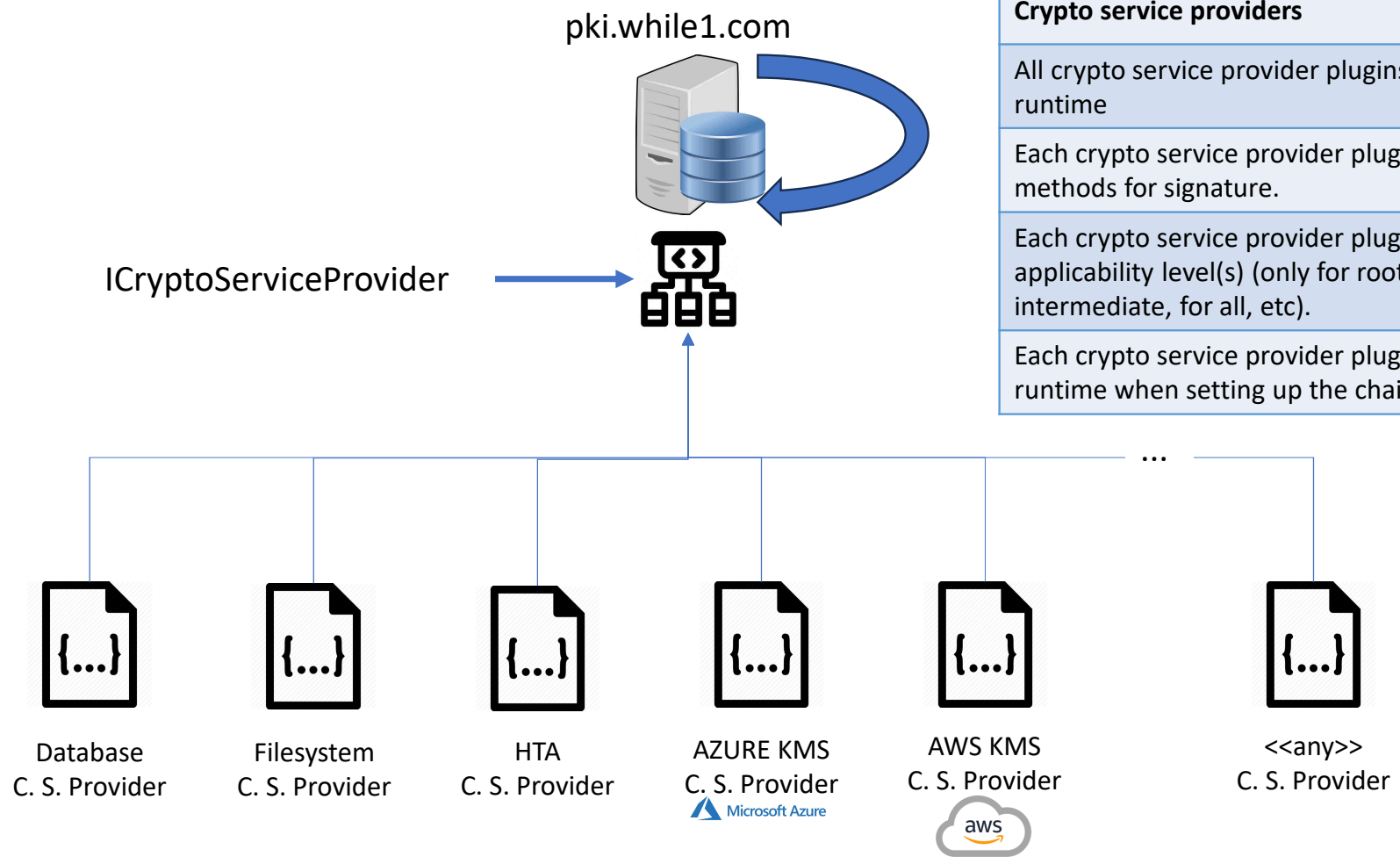
Reachability according to customer design

Multiplatform capability

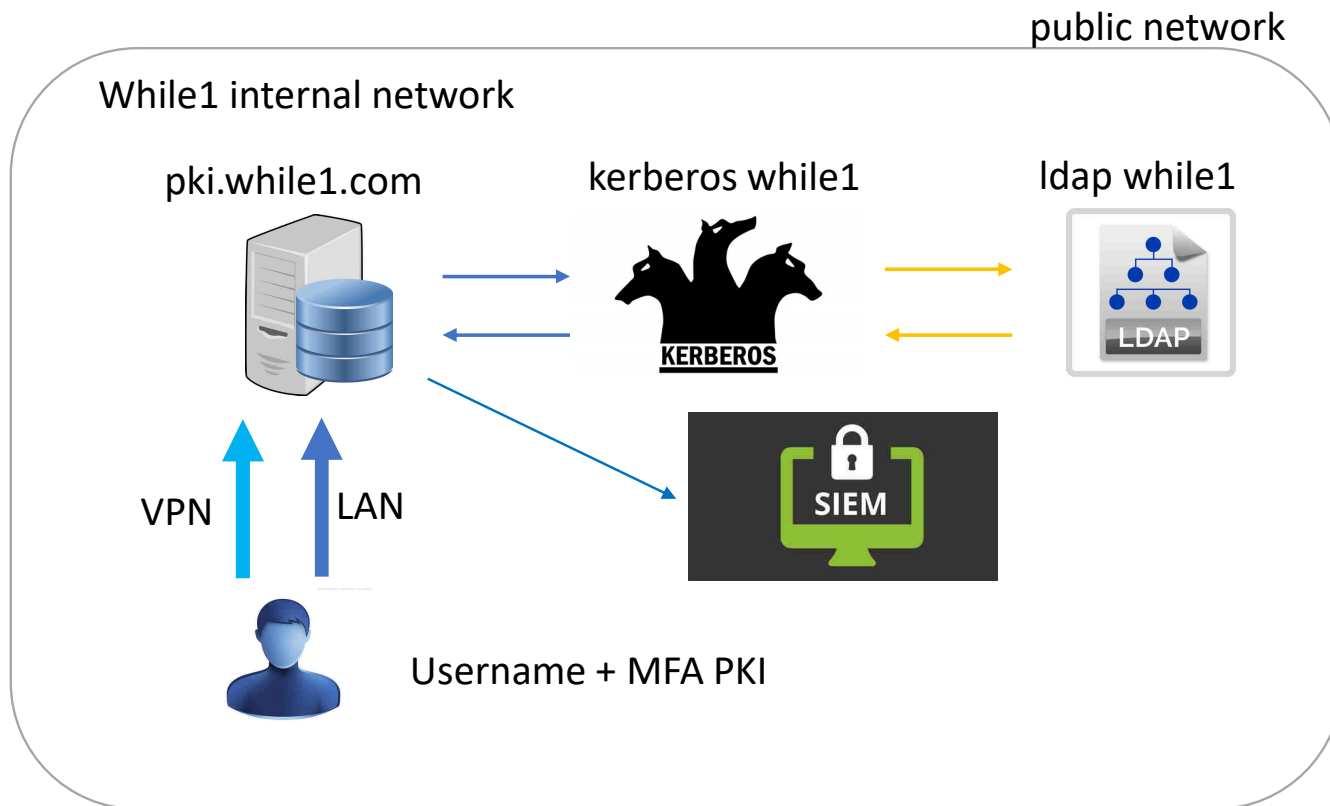
Siem feeder

Physical installation or contained installation as well





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.



### HIGH LEVEL PROPERTIES

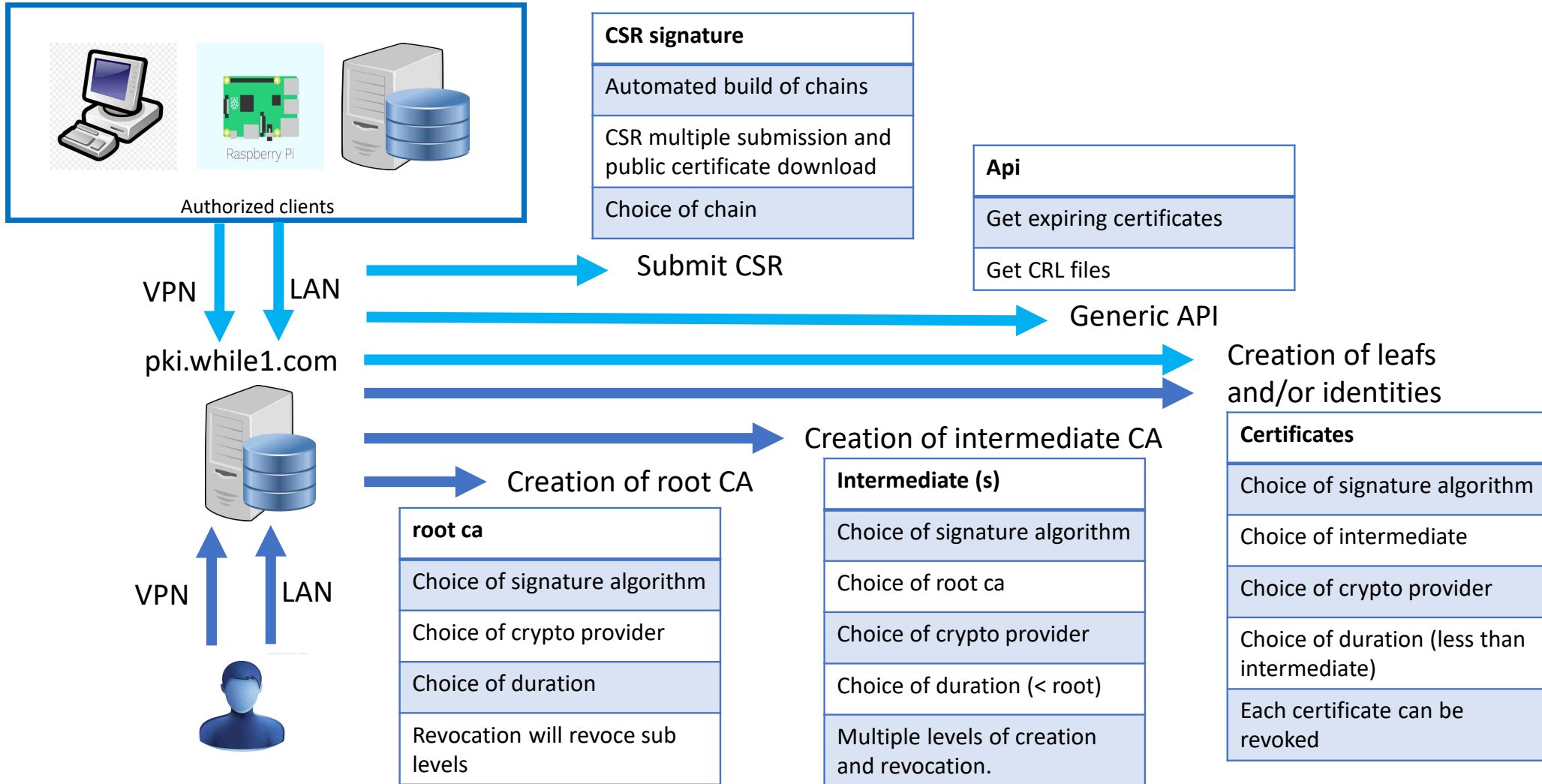
Integrated with internal security provider

Not exposed to internet

Multiplatform capability

Siem feeder

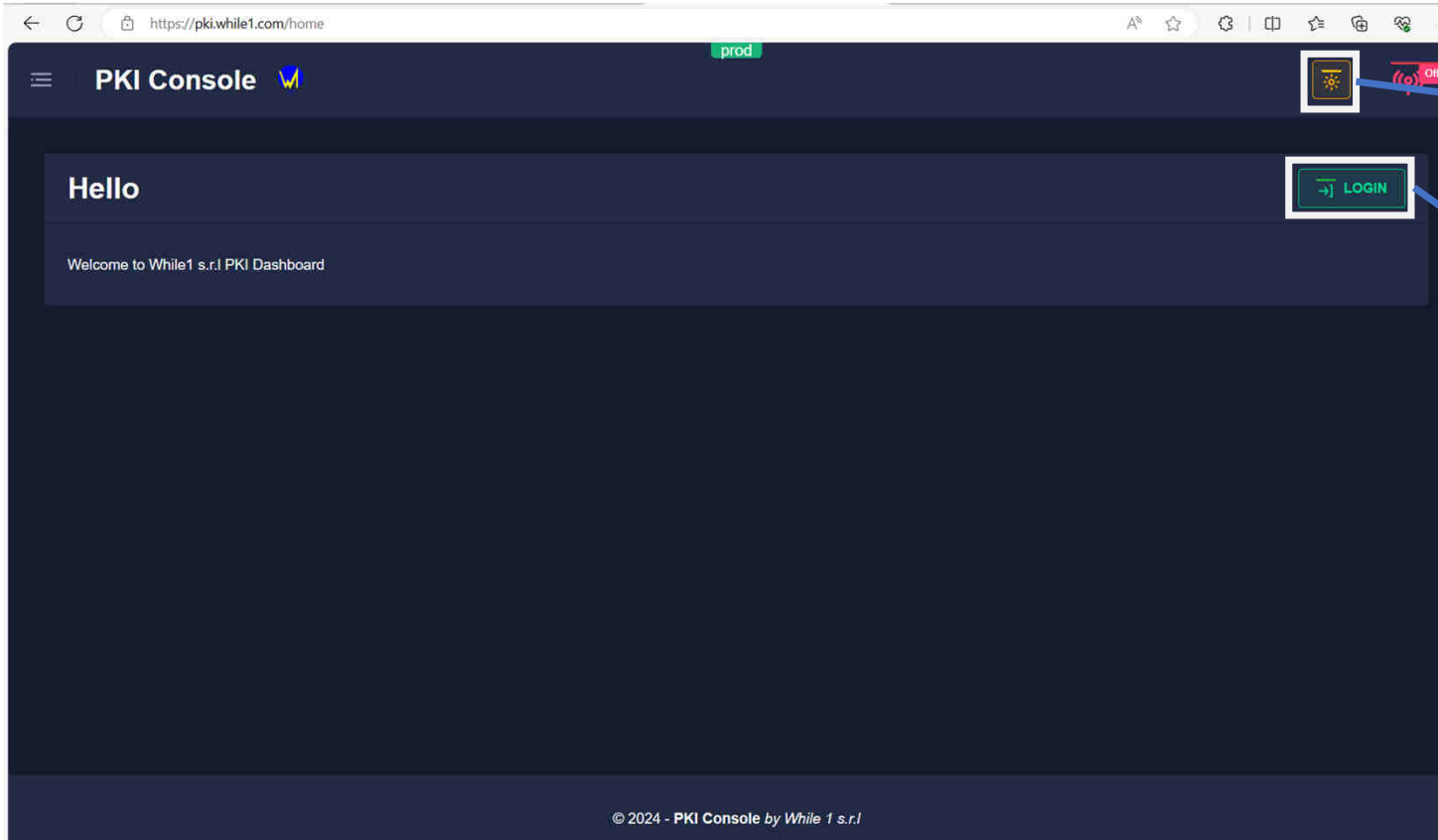
Physical installation or contained installation as well







while1.com // PKI >> Welcome page



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



Reference to logged user

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



while1.com // PKI >> root and intermediates

The screenshot shows the PKI Console interface. At the top, there is a navigation menu with options like Home, Certificate Authorities, Issued Certificates, etc. Below the menu is a search and filter section with a 'RELOAD' button and a 'SHOW ADVANCEDSEARCH' button. A list of filterable fields is shown, including id, certificateScope, commonName, serialNumber, issuer, deleted, certPEM, createdByUser, keySize, keyAlgorithm, hashAlgorithm, expiryDate, thumbprint, source, lastChangeAt, description, hierarchyLevel, assignedCRLUrls, and privateKeyAddressId. Below the filters is an 'ADD' button and a table of certificate authorities. The table has columns for Actions, ID, CERTIFICATESCOPE, COMMONNAME, SERIALNUMBER, and ISSUER. The first row is for an issuer, the second for a root, and the third for an internal authority. The 'ADD' button is highlighted with a red box, and the 'ISSUER' column for the root certificate is highlighted with a red box. The 'ISSUED BY' field for the internal authority is highlighted with a red box.

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
	61a33995-9896-4780-88af-	issuer.crl.while1.com	CN=issuer.crl.while1.com	1F7DF66D4DEEB75DF31B03D31F58241F	Root
	bb2da3f6533326e3c5eca4bd-4abf-h055-	root.while1.com	CN=root.while1.com	1F790E029A882B04C522B07589E9E21F	Root
	e7fe87a2beffc9635df7-287f-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

PKI Console

Home

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

RELOAD

ADD

Actions

MEMBER	ISSUER
EB75DF31B03D31F58241F	Root
B2B04C522B07589E9E21F	Root

Issued By : Root.While1.Com

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, KeyAlgorithm, 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 developed 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

The screenshot shows the PKI Console interface with a confirmation dialog box open. The dialog is titled "Revoking issuer.crl.while1.com" and contains the following text:

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

The dialog is overlaid on a table of certificate authorities. The table has columns for ID, Issuer, and Issued By. The first row is highlighted in red, indicating it is the selected item for revocation.

ID	Issuer	Issued By
61a3399-9896-4788af-bb2da3f-26e3c5e	issuer.crl.while1.com	Root
a4bd-4abf-b055-e7fe87a2beff	root.while1.com	Root
c9635df7-287f-4766-a499-3de9798c4d6c	internal.while1.com	Root

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

PKI Console

LeafCertificates

RELOAD SHOW ADVANCEDSEARCH

id  certificateScope  commonName  serialNumber  issuer  deleted  certPEM  createdByUser

keySize  keyAlgorithm  hashAlgorithm  expiryDate  thumbprint  source  lastChangeAt

description  hierarchyLevel  assignedCRLUrls  serialAlgorithm

ADD

Items per page: 10 1 - 1 of 1

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
	8bf2e7d8-af13-4451-a572- e4b0bcb007f1	pki.while1.com	CN=pki.while1.com	1FE34A4F182CB6075B3588345C157A1F	Issued By : Internal.While1.Com

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

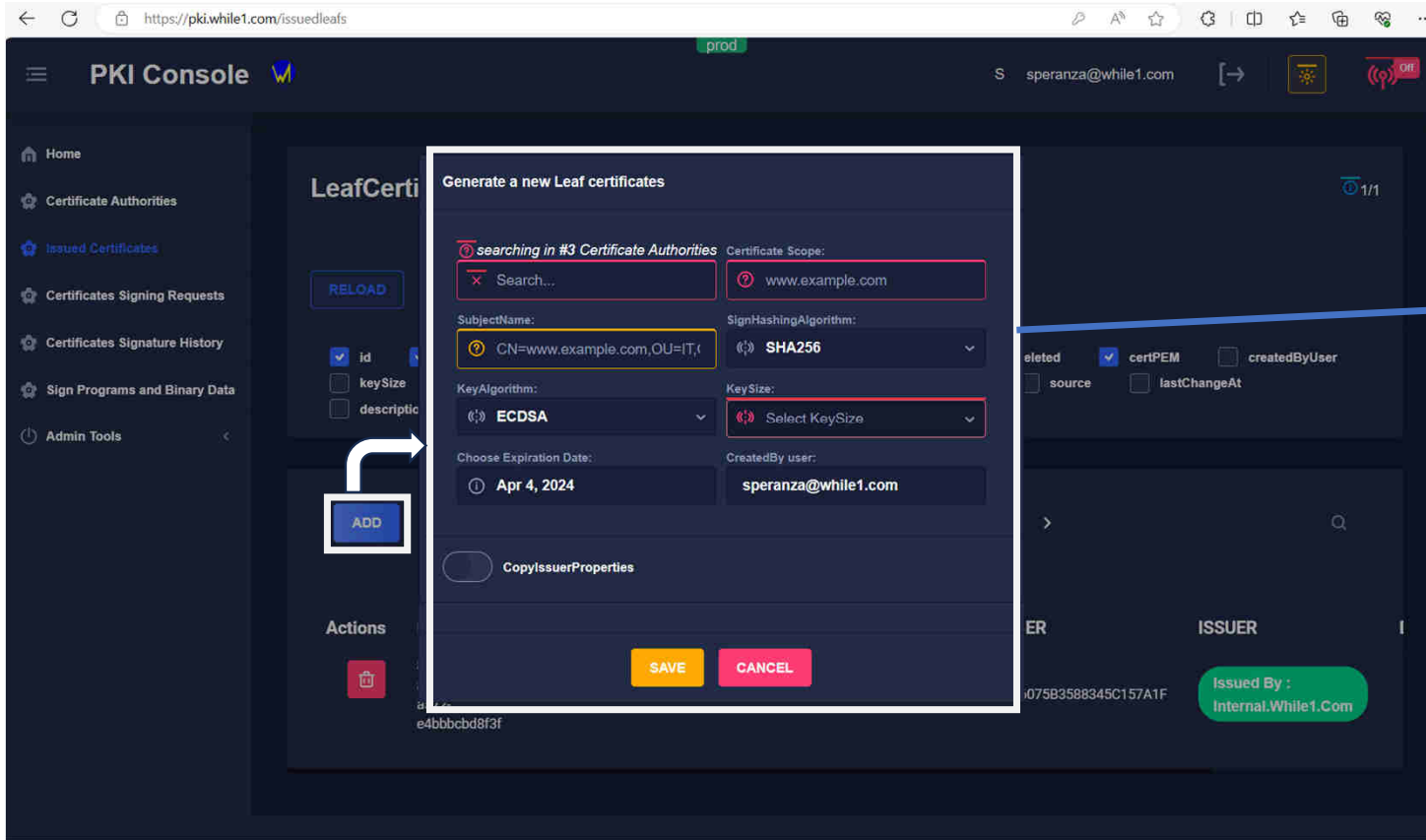
Button to add a leaf certificate. Explain in the next slide

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



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, KeyAlgorithm, 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

The screenshot shows the PKI Console interface with a dialog box open. The dialog box contains the following text: "You are about to revoke certificate pki.while1.com (1FE34A4F182CB6075B3588345C157A1F) . Are sure you want to proceed? (this action cannot be undone)." Below the text are two buttons: "CONFIRM" (green) and "CANCEL" (red). A blue arrow points from the dialog box to the right, and a white arrow points from the dialog box to the "Actions" column of the table below.

Actions	ID	CERTIFICATESCOPE	COMMONNAME	SERIALNUMBER	ISSUER
	8bf2e7d8-af13-4451-a572-e4bbcbcd8f3f	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.





The screenshot shows the 'App Logs' page in the PKI Console. The interface includes a sidebar with navigation options like Home, Certificate Authorities, Issued Certificates, etc. The main content area has a search bar with 'CLEAR SEARCH', 'RELOAD', and 'ADVANCED SEARCH' buttons. Below the search bar are checkboxes for various log fields: id, timeStamp, level, message, requestid, messageTemplate, exception, logEvent, actionName, machineName, user, clientAddress, userAgent, and userRoles. A table below shows log entries with columns for ID, TIMESTAMP, LEVEL, MESSAGE, REQUESTID, and MESSAGETEMPLATE. The table shows three entries with IDs 1656, 1655, and 1654.

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 is meant for administrative purposes only.



while1.com // PKI >> user management

PKI Console

prod

S speranza@while1.com

RELOAD

userDomain ssoUserName enabled appUserId description

Filter by Enabled

Show All

ADD USER

Items per page: 10 1 - 4 of 4

Actions	USERDOMAIN	SSOUSERNAME	ENABLED	User Info	DESCRIPTION
	WHILE1.COM	GUIDICE	<input checked="" type="checkbox"/>	<a href="#">GUIDICE@WHILE1.COM</a> 0d8b79bb-F1cd-4275-9094-E93580feb34b	1 CLAIMS Enabled by havugukuri@while1 at 04/04/2024 10:3: +00:00
	WHILE1.COM	SPERANZA	<input checked="" type="checkbox"/>	<a href="#">SPERANZA@WHILE1.COM</a> 4d6fc387-Bfd5-49e9-997e-Aae6a3532b65	1 CLAIMS Enabled by havugukuri@while1 at 04/04/2024 10:3: +00:00
	WHILE1.COM	HAVUGUKURI	<input checked="" type="checkbox"/>	<a href="#">HAVUGUKURI@WHILE1.COM</a> 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 is meant for administrative purposes only.



while1.com // PKI >> apis

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.

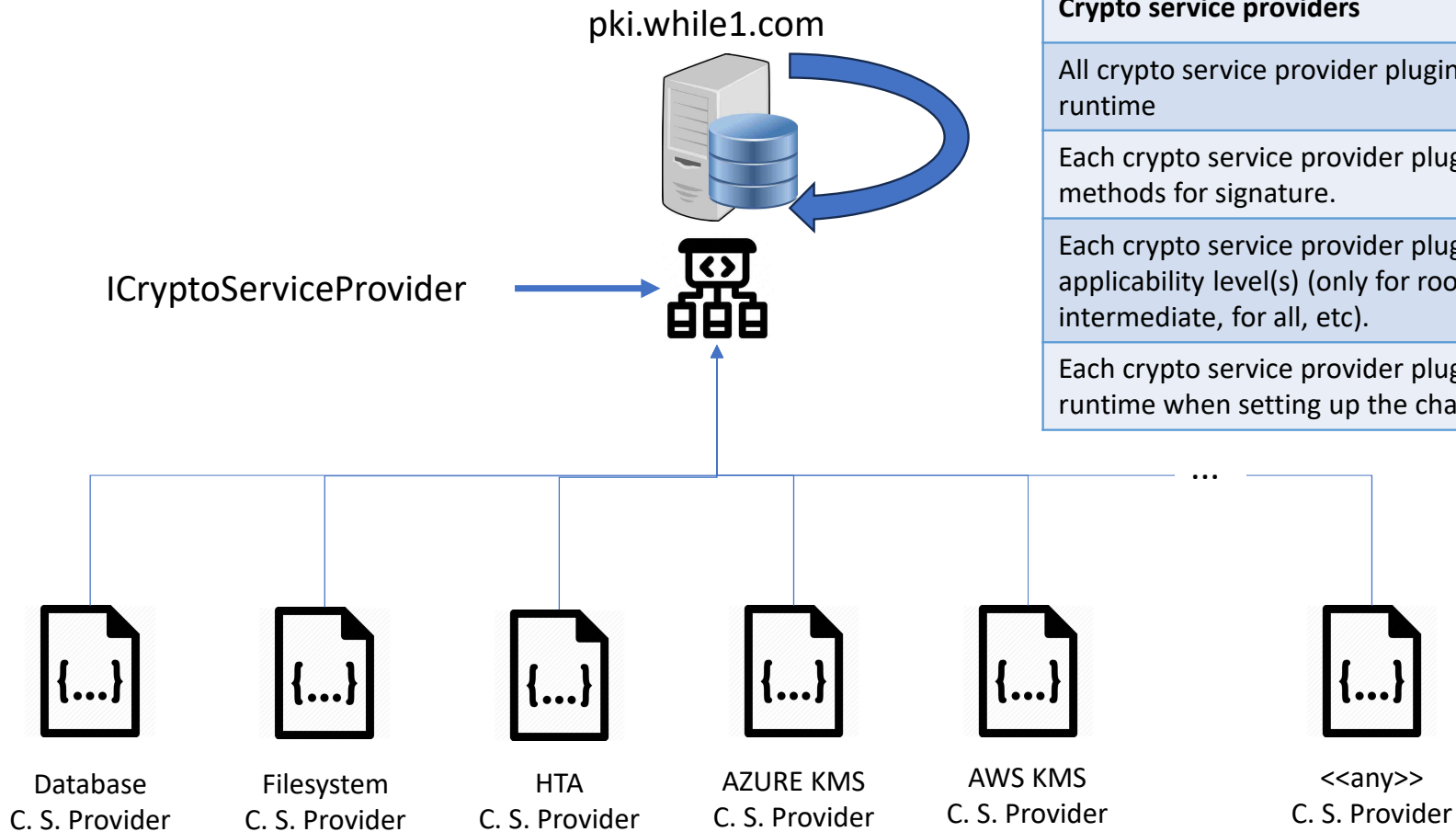


**WHILE 1**  
**SOFTWARE**

Project	Internal deployment	Platform
PKI	Yes	Windows / PostgreSQL



Version	Deployed on	Changelog	Confidentiality Level
V0.9.432 78	April, the 3 <sup>o</sup> , 2024	First initial release. Local authentication. Root ca, intermediate ca, leafs, choice between different algorithm and different providers	GENERAL BUSINESS



**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.