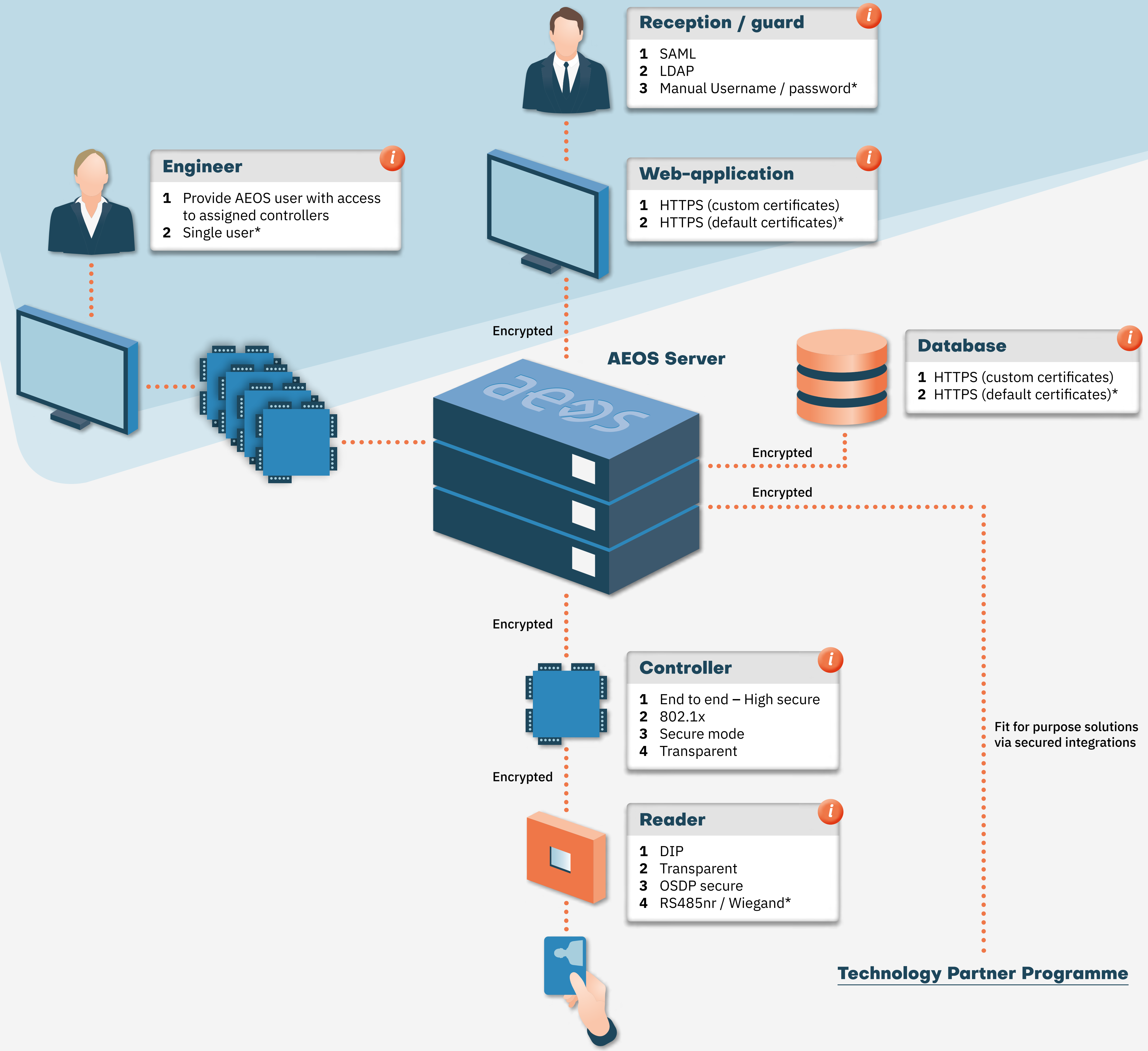
AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

Technology Partner Programme

* Default

aeos

Integrations support a variety of security possibilities

In AEOS core:

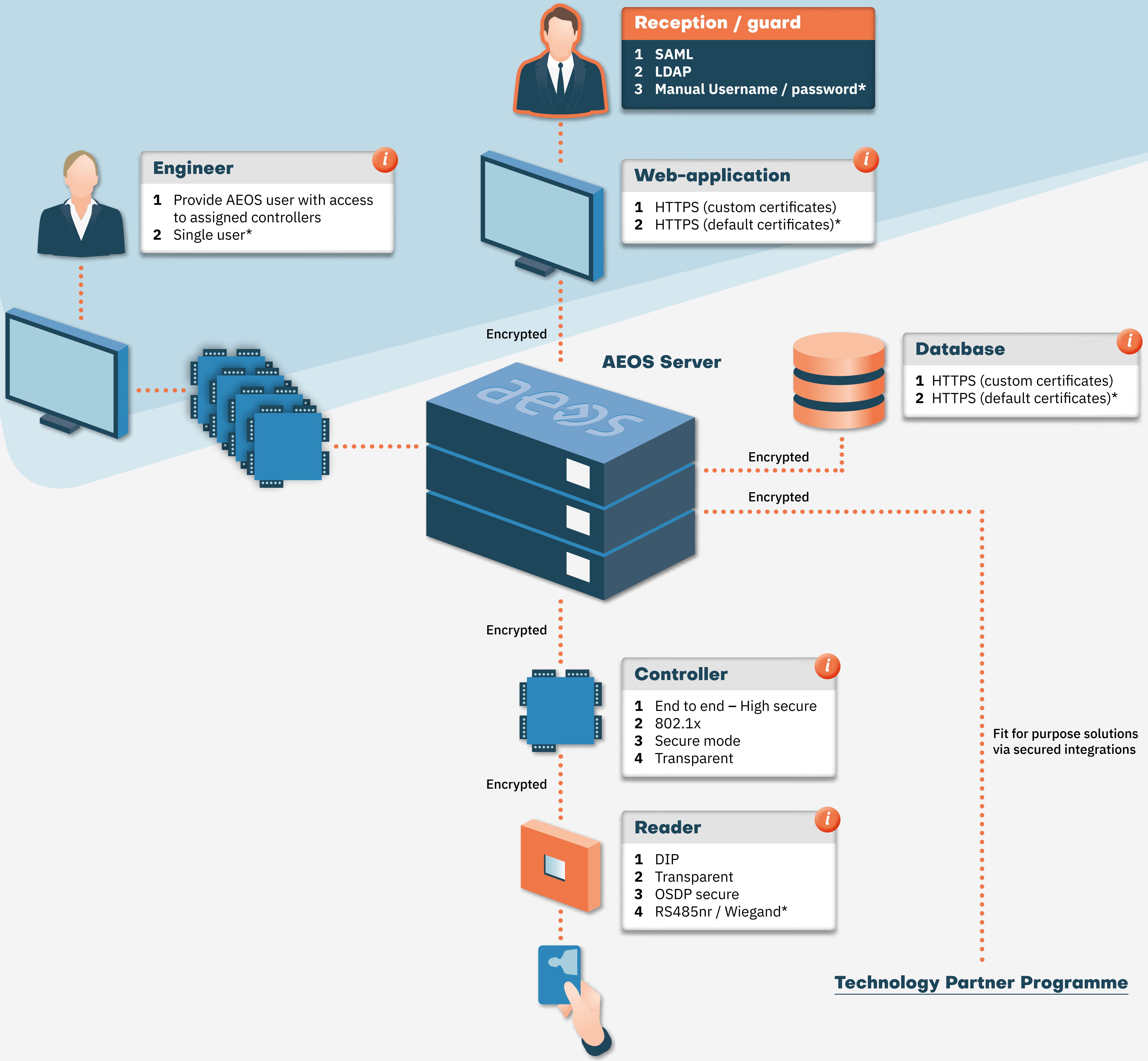
- Physical Access Control
- Locker Management
- Intrusion Detection

Integrations via the Technology Partner Programme:

- Readers
- Wireless locks
- Key cabinets
- Physical Security Information Management (PSIM)
- Video Management
- Intercom Elevators Fire
- Mobile access
- Biometrics

nedap

AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Encrypted

AEOS Server

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Encrypted

Encrypted

Encrypted

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Encrypted

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

Fit for purpose solutions via secured integrations

Technology Partner Programme

* Default

Reception / guard

1 SAML

Security Assertion Markup Language
With the use of SAML, an external Identity Provider can be added between client workstation and the AEOS server. Providing you additional login functionalities like two-factor authentication via for example Okta.

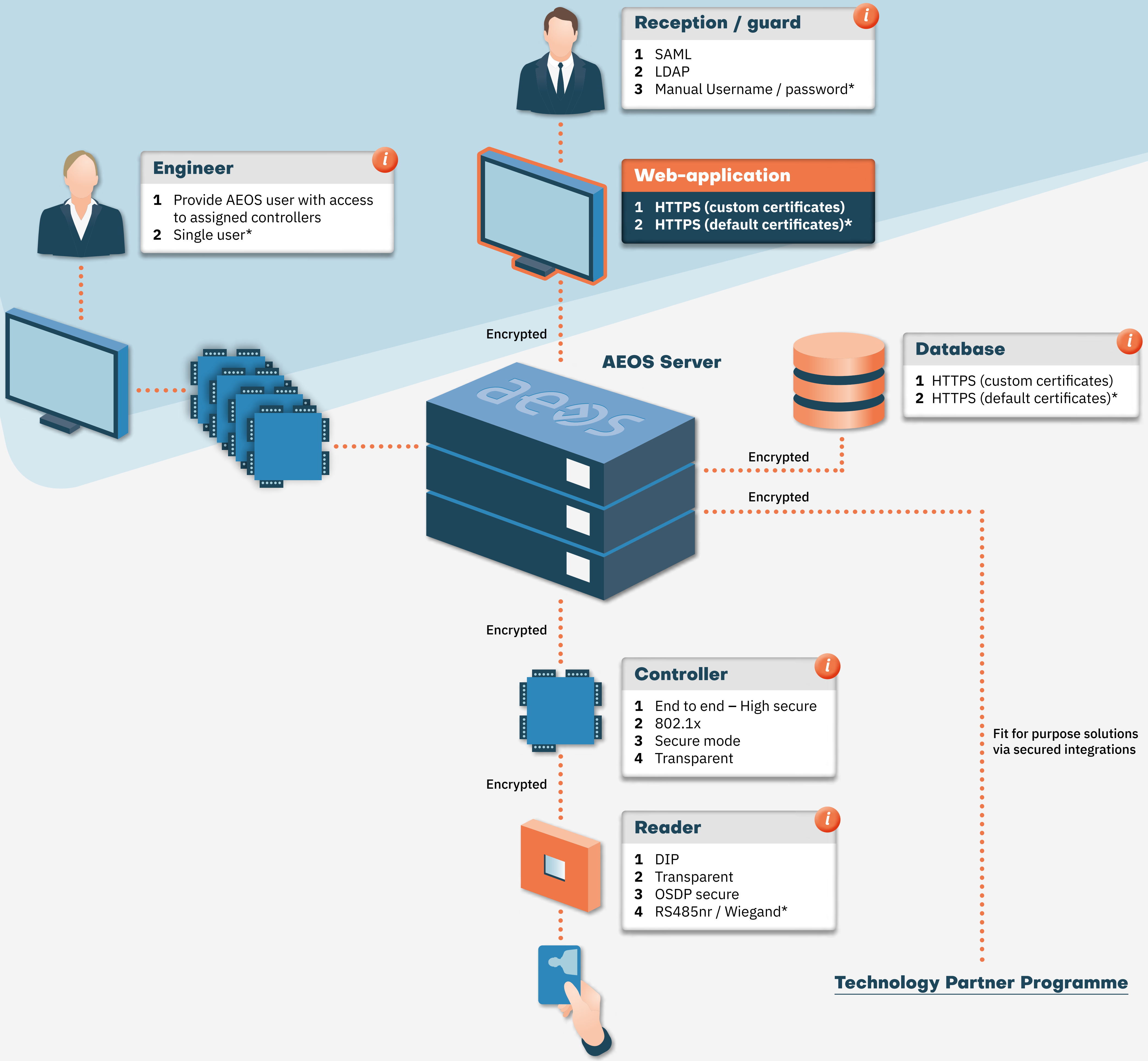
2 LDAP

Lightweight Directory Access Protocol
With the use of LDAP, you can allow access to AEOS for users with their Windows login credentials. This can be configured to Single Sign On as well.

3 Manual Username / password*

By default, AEOS users are manually created giving people access with username and (strong) password.

AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

Technology Partner Programme

* Default

Web-application

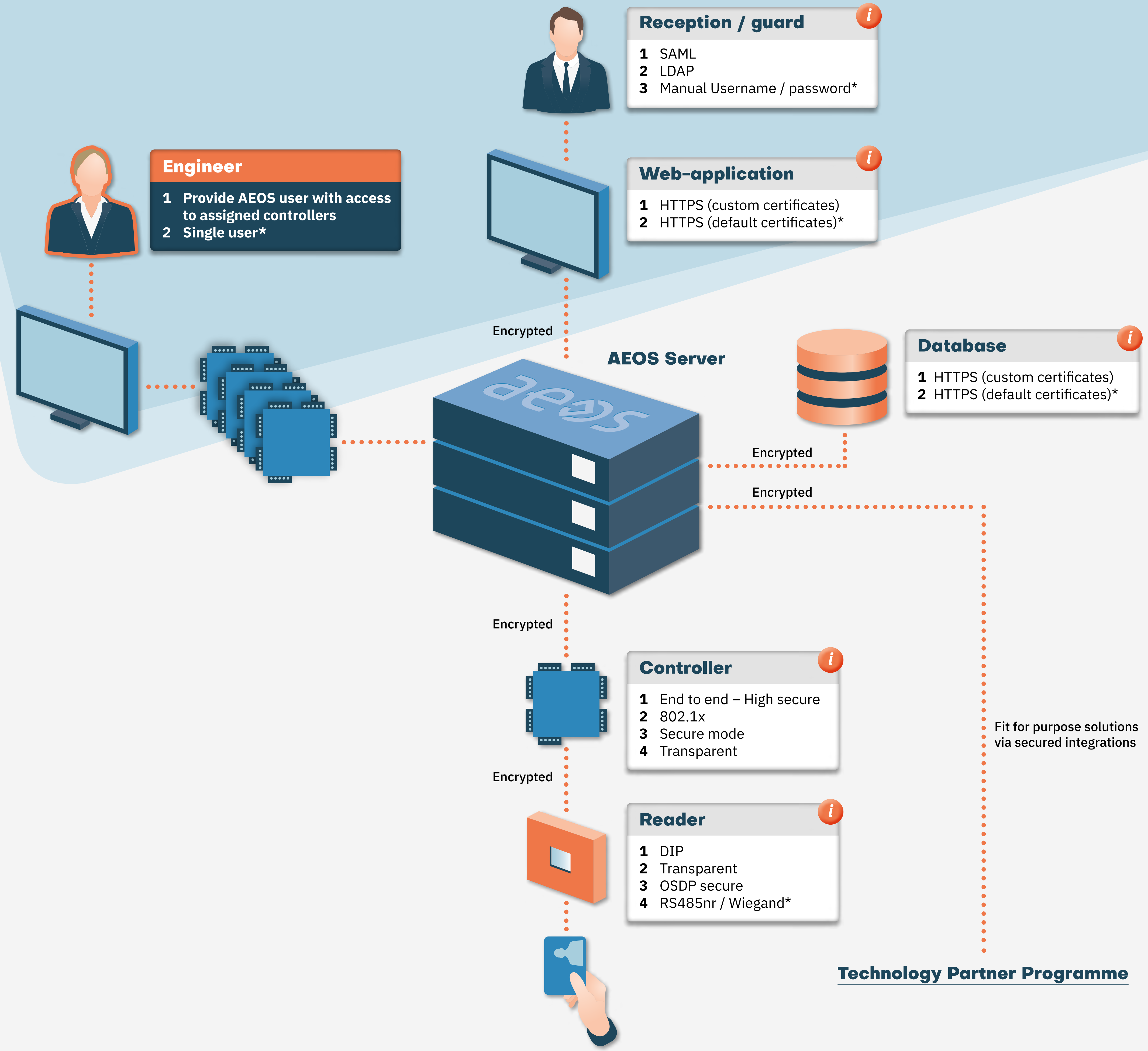
1 HTTPS (custom certificates)

The communication between client workstation and server is secured via self-signed certificates using TLS. This can be customized to customer specific certificates.

2 HTTPS (default certificates)*

By default, after an AEOS installation.
The communication between client workstation and server is secured via self-signed certificates using up-to-date TLS versions.

AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard
1 SAML
2 LDAP
3 Manual Username / password*
Engineer
1 Provide AEOS user with access to assigned controllers
2 Single user*
Web-application
1 HTTPS (custom certificates)
2 HTTPS (default certificates)*
Encrypted
AEOS Server
aeos
Database
1 HTTPS (custom certificates)
2 HTTPS (default certificates)*
Encrypted
Encrypted
Encrypted
Controller
1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent
Encrypted
Fit for purpose solutions via secured integrations
Reader
1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*
Technology Partner Programme

* Default

Engineer

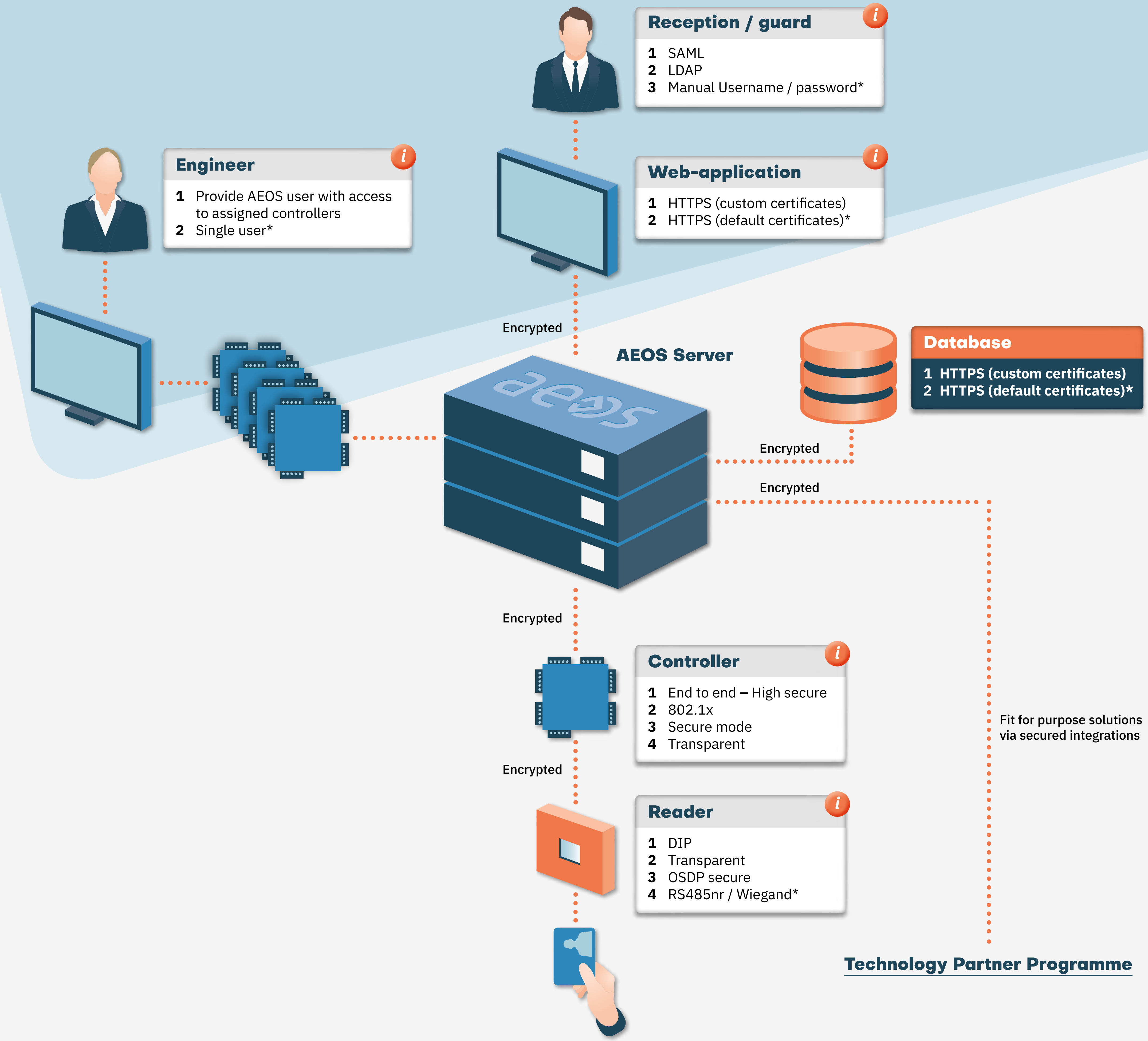
1 Provide AEOS user with access to assigned controllers

You can give AEOS system users access rights to login on an AEpu using their AEOS user name and password. This allows you to give users access to the for them relevant controller and log their personal activities on the controllers.

2 Single user*

By default, AEOS comes with a pre-configured single username/password for all controllers. The password can be changed, but username stays the same.

AEOS cybersecurity: high-level protection against physical & digital threats



Encrypted
AEOS Server
aeos
Encrypted
Encrypted
Encrypted
Encrypted
Fit for purpose solutions via secured integrations
Technology Partner Programme

Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

* Default

Database

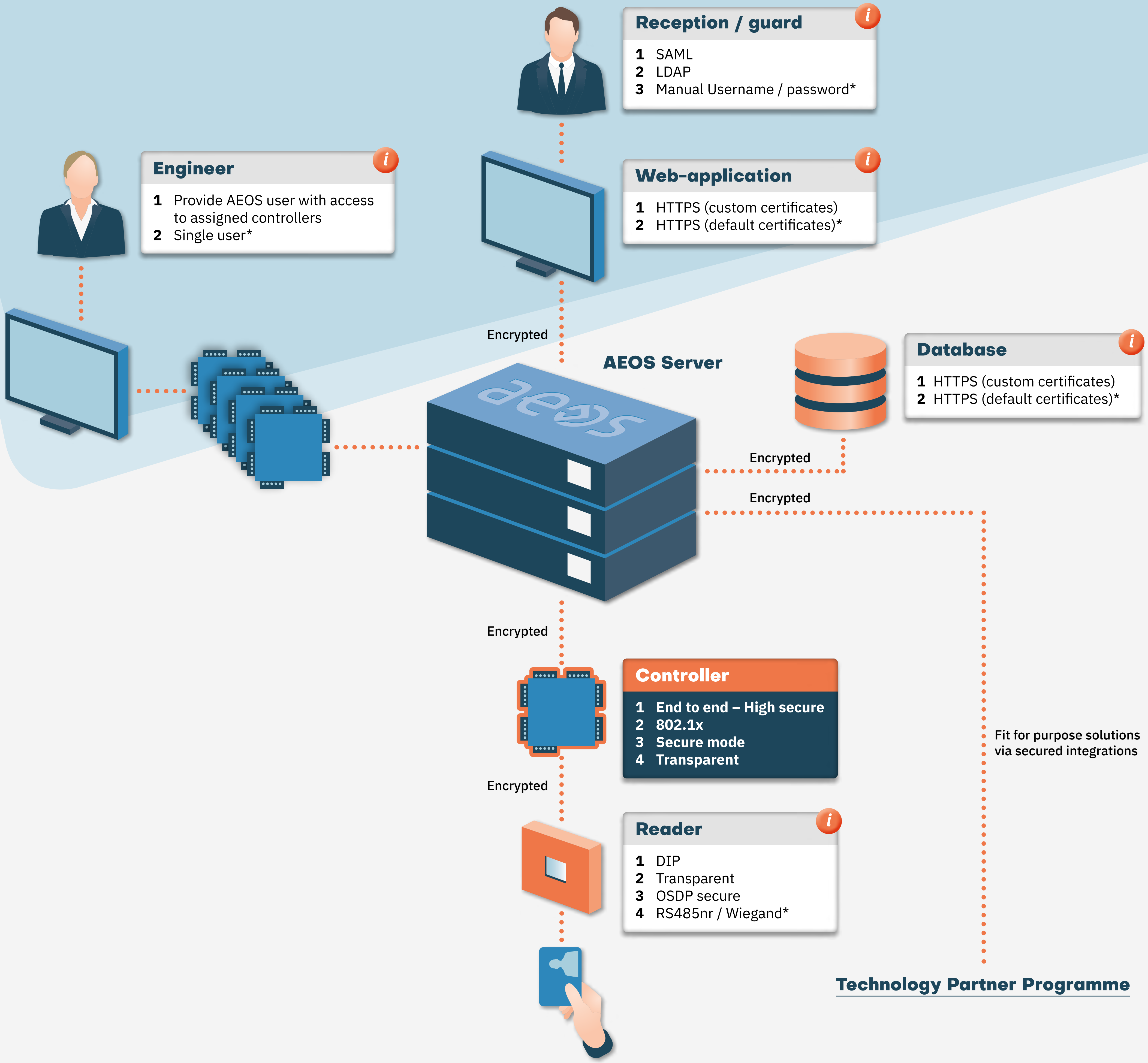
1 HTTPS (custom certificates)

Similar to the HTTPS security at the client workstation. The communication between AEOS and Database can be secured via TLS as well. This is done via provided certificates by the setup (self-signed), or with customer specific certificates.

2 HTTPS (default certificates)*

Similar to the HTTPS security at the client workstation. The communication between AEOS and Database can be secured via TLS as well. This is done via provided certificates by the setup (self-signed).

AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Encrypted

AEOS Server

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Encrypted

Encrypted

Encrypted

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Encrypted

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

Fit for purpose solutions via secured integrations

Technology Partner Programme

* Default

Controller

1 End to end – High secure

In addition to the secure mode below in option 3. To alternate and manage the certificates on Nedap controllers, you require a Certificate Management Server. This server manages and distributes the certificates to all Nedap controllers, and stores them on a SAM (Secure Access Module) which is placed in the controller.

2 802.1x

The 802.1x is a industry standard protocol to allow you to authenticate devices connected to your network. A connection with the network is only allowed after the protocol trusted the relation (based on certificates) between the device (Nedap controller) and the authentication server. The authentication server is arranged and managed by customers IT department.

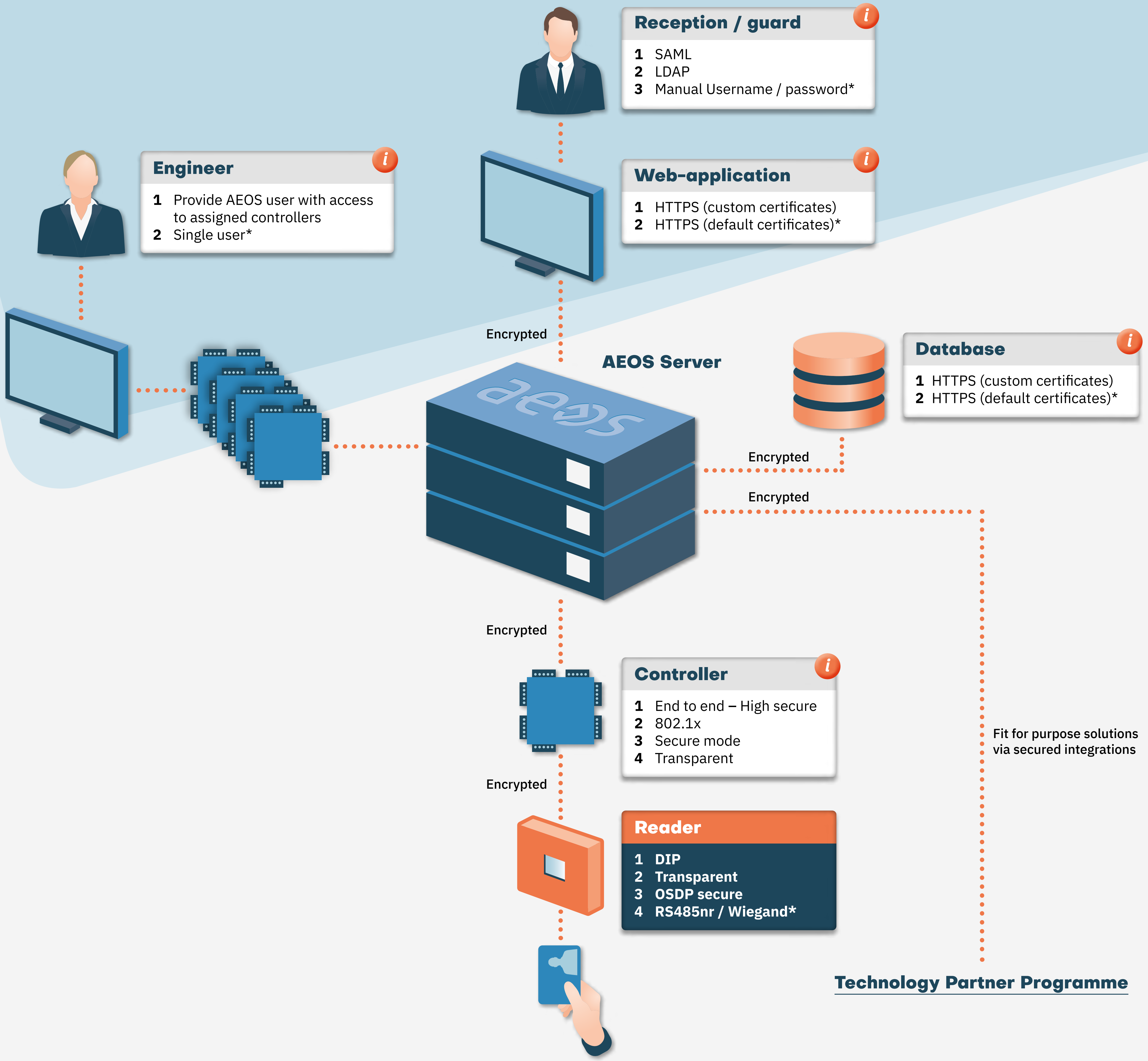
3 Secure mode

Within every AEOS installation, you have the option the enable secure mode. This enables a secured TLS connection based on Nedap provided certificates between the AEOS server and Nedap controllers.

4 Transparent

In common practice Access control, the reader contains card data like card keys to decrypt the card. This means your card data is placed outside your building in the readers. By setting the reader to transparent mode, you shift all sensitive card data from the reader to the controller. And hereby to the safe side of the door. All decrypting of card data is done in the controller itself. To support this, the controller must be configured in Transparent as well.

AEOS cybersecurity: high-level protection against physical & digital threats



Reception / guard

1 SAML
2 LDAP
3 Manual Username / password*

Engineer

1 Provide AEOS user with access to assigned controllers
2 Single user*

Web-application

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Database

1 HTTPS (custom certificates)
2 HTTPS (default certificates)*

Controller

1 End to end – High secure
2 802.1x
3 Secure mode
4 Transparent

Reader

1 DIP
2 Transparent
3 OSDP secure
4 RS485nr / Wiegand*

* Default

Reader

1 DIP

This is a (by Nedap created) open standard to create communication between the Nedap controller and readers or scanners. This communication can be done over TCP/IP (or in the future rs485).

2 Transparent

In common practice Access control, the reader contains card data like card keys to decrypt the card. This means your card data is placed outside your building in the readers. By setting the reader to transparent mode, you shift all sensitive card data from the reader to the controller. And hereby to the safe side of the door. All decrypting of card data is done in the controller itself.

3 OSDP secure

One of the most used industry standards for readers. Via OSDP you can connect third-party readers to Nedap controllers. OSDP also has the possibility to encrypt the communication via OSDP secure. The encryption is done via a so called ‘Encryption key’ of 32 character long.

4 RS485nr / Wiegand*

RS485NR
Nedap’s standard for our own reader portfolio. Secured via RC4 encryption.

Wiegand
Probably the most known industry standard protocol if it comes to readers. But also the most insecure protocol as Wiegand doesn’t have any encryption or security.