XFS4IoT SP-Dev Workgroup

3rd September 2024

Confidential

- Post-break recap from previous meetings
- Presentation from SBS
- SP-Dev framework update
- What's next?
- Next meeting

Recap from previous meetings

- Migration to 2023-2
  - — Framework and samples migrated
  - — Template package version 2.0.1 published
  - — New features added
    - StatusChanged event in all device interfaces
    - New commands in KeyManagement interface
    - Camera support
      - Including SP sample and SP support in test client application
    - Check Scanner support
      - Including SP sample and template
  - — .NET 8 and C# 12

Recap from previous meetings

- Demos
  - — Migration of existing code to 2023-2
  - — Camera SP with low-cost hardware (Raspberry Pi)
  - — Check Scanner SP
  - — Creating a complete camera SP with the code template
  - — Camera SP on Android phone
  - — Card reader, Receipt printer and Pinpad on POS device

Recap from previous meetings

- Guest speakers
  — First National Bank (FNB) in South Africa
    - Collaboration with Hyosung
    - Using the framework to create SPs
    - Running SPs on Windows and Linux
    - Discussed challenges and shared tips for XFS4IoT adoption

  — Synaforce in Germany
    - Presented cloud-based ATMs project at Shell stations
    - Reduced hardware footprint
    - Improved flexibility and provided new transactions
    - Discussed challenges and plans for the future

XFS4IoT SP-Dev Workgroup
3rd September 2024

Thomas Eder

SBS
Salzburger Banken Software

SBS Overview

Founded in 1988 in Austria, headquartered in Salzburg, branch offices Germany and Switzerland

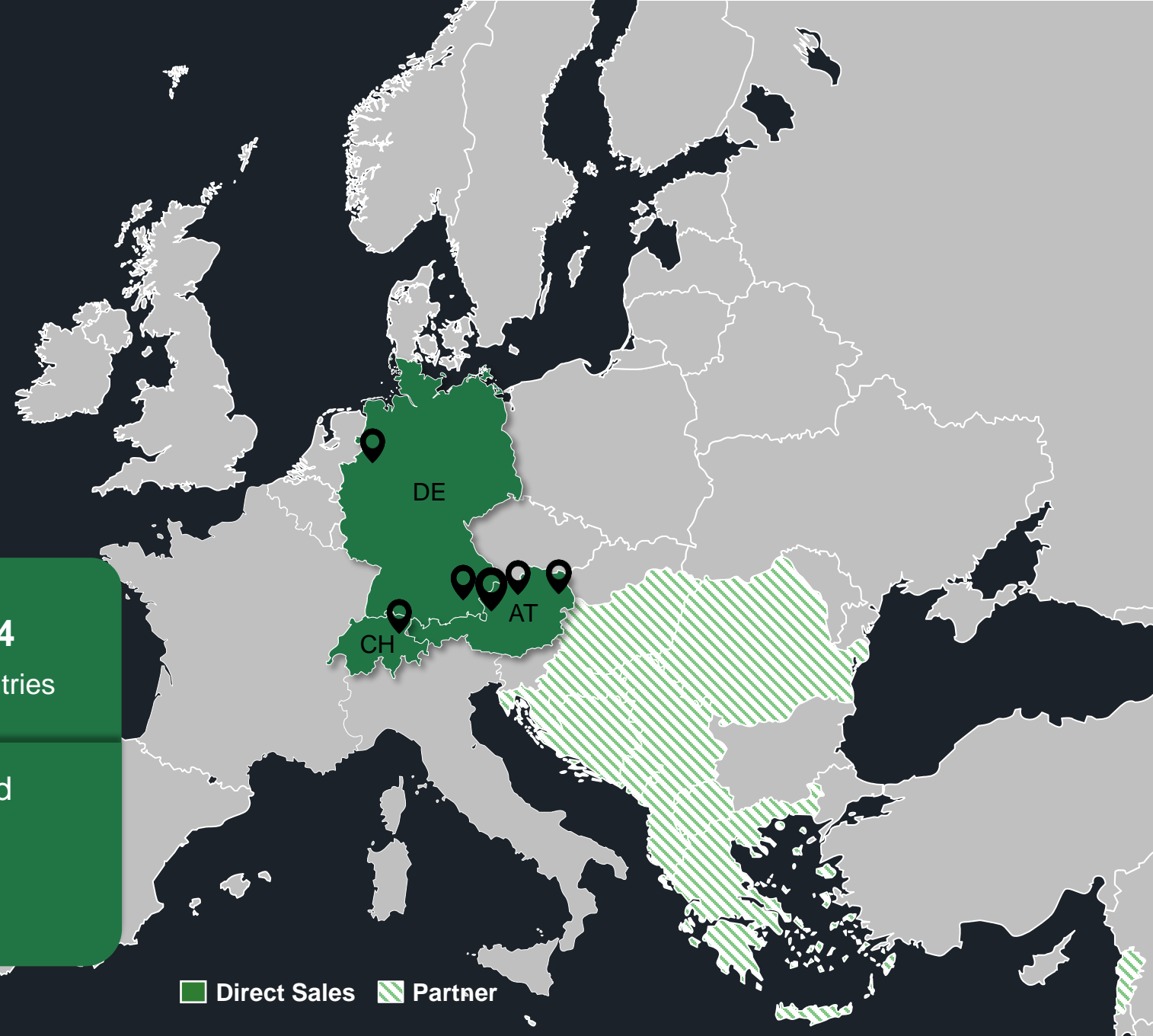Owner-managed, 100+ employees

66,000+
Self-service terminals

140+
Terminal models and variations

14
Countries

Multivendor software solutions and managed services for self-service terminals

Market leader in ATM software in the DACH region

DE

CH

AT

☐ **Direct Sales**   ▨ **Partner**

DK - GBIC

DK = Deutsche Kreditwirtschaft = GBIC = German Banking Industry Committee

- Until 2011 known as ZKA (Zentraler Kreditausschuss)

- Consortium of the top five financial institutions in Germany
  (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken,
  Bankenverband, Finanzgruppe Deutscher Sparkassen- und Giroverband,
  VÖB – die öffentlichen Banken, vdp – Die deutschen Pfandbriefbanken)

- Publishes a set of rules and procedures for the German ATM system.

- This is to ensure that the banking client has the same high standard of security and service on all participating ATMs.

- Homepage: https://die-dk.de

DK-Specifications

- The basic specification is the so-called "GA Vereinbarung" concerning cashout transactions (including NFC based transactions):

  „Anlage 3 zur Vereinbarung über das Deutsche Geldautomaten-System"
  - about 600 pages in German

- Additional important specifications (in German):

- OPT – „Online Personalisierung von Terminals" for encryption and key exchange

- PIN-Management – for activating and changing PINs

- Geldkarte (outphased with 2025) – for cashless payment of goods and services using an electronic purse

DK Certification

- German approval necessary for cashout, OPT and Geldkarte

- Mandatory for every terminal-vendor and every combination of
  EPP-type + contactbased card reader type + contactless card reader type

- Up to now, SBS has received more than 30 DK-certificates, about a dozen per terminal vendor

- Special additional requirements for PCI and EMVCo Level1 and Level2 for both contactbased
  and contactless Hardware and Software have to be met.

- E.g.:
  PCI 5.x for EPP (PinPad)
  EMVCo L1 4.3 (Card Reader – contact based)
  EMVCo L2 4.3 (L2-Software – contact based)

DK and XFS

SecureMsgSend / SecureMsgReceive

- PinPad-XFS-Interface was extended for DK-functionality

- Main extension: new SecureMsgSend / SecureMsgReceive commands

- Important command parameter: protocol

- Cashout: protocol genAs to generate / verify host messages

- OPT (key management):
  protocol isoPS to generate / verify host messages,
  protocol hsmLdi to read key management data

- PIN-Management:
  protocol pinCmp to save and compare new and old PIN and to get PACs (encrypted PINs)

DK and XFS

Other Commands

- SetHSMTData:
Write special terminal configuration data to the EPP, which is used to create/verify host messages (OPT, Geldkarte)

- GetHSMTData:
Read special terminal configuration data from the EPP, which is used to create/verify host messages (OPT, Geldkarte)

- HSMInit:
Reset/delete OPT keys in the EPP

DK and XFS4IoT

Overview

- PIN-subgroup (Seishi Nakano) works on drafting DK-interface for the XFS4IoT-specification

- Proposal of DK interface specification in progress

- Goal: minimum set of commands and events to adhere to DK-specifications and for DK-certification

DK and XFS4IoT

Modifications / Status

- Renaming from ZKA/DK to German
  - „German Specific Interface"

- Geldkarte was removed (phased out 2025)

- References cleaned up and updated

- Unused interface parts removed (commands, parameters, parameter values)

- Status: main part done, now further reviews in PIN-subgroup

XFS4IoT SP-Dev Workgroup
3rd September 2024

Thomas Eder

Thank you for your attention!

SP-Dev Framework v2.4

Updates in SP-Dev Framework v2.4

- Corrected KeyManagement capabilities LoadCertificateSigner options to match XFS4IoT 2023-2 Specification

- Supported validating partial counts in CashDispenser.Dispense

- Corrected issue with VendorMode Inactive state on StatusChangedEvent

- Add Auxiliaries UPS status Good

- Updated GetCashStorageConfiguration and GetCheckStorageConfiguration to allow the service to return null when storage is not detected

- Support returning Chip ATR response on CardReader.ChipPower command
  — Added in XFS4IoT specification 2023-2

- Improved Denominate and Dispense commands performance with large amounts

Updates in SP-Dev Framework v2.4

- Added support for CheckUnit lights added in XFS4IoT 2023-2

- Added support for target position Reject for CashManangement.CalibrateCashUnit and CashDispenser.TestCashUnits

- Relaxed parameter checks for CardReader.Reset command
  — Ignore application provided storage id when media is ejected or no action is performed

- Correct RetractArea handling for CashManagement.Retract command

- Update KeyManagement command capabilities to include ExportRSADeviceSignedItem

- Correct Camera status reporting to handle multiple camera from the same service correctly

- Update Keyboard DataEntry, PinEntry and SecureKeyEntry commands to return KeyNotSupported error code.

- Updated message header to include below fields

  — Status for Acknowledgement messages

  — CompletionCode for Completion messages

  — ErrorDescription for Completion messages

Command header

2021-1 command header:

```
"header":
{
    "type": "command",
    "name": "Common.Status",
    "requestId": 12345,
}
```

2023-2 command header:

```
"header":
{
    "type": "command",
    "name": "Common.Status",
    "version": "2.0",
    "requestId": 12345,
    "timeout": 1000
}
```

Completion header

2021-1 completion header:

```
"header":
{
    "type": "completion",
    "name": "Common.Status",
    "requestId": 12345,
}
```

2023-2 completion header:

```
 "header":
{
    "type": "completion",
    "name": "Common.Status",
    "version": "2.0",
    "requestId": 12345,
    "completionCode": "fraudAttempt"
    "errorDescription": "Error text"
}
```

Comparing SP-Dev Framework versions

- Changes on GitHub

- Compare between releases

- Shows all commits between package versions

https://github.com/KAL-ATM-Software/KAL_XFS4IoT_SP-Dev/compare/v2.3.0...v2.4.0

What's next?

Demos, POCs and guest speakers

- TLS demo

- Framework updates and roadmap

- CEN Specification update

- More guest speakers

- More demos

Zoom

- First Tuesday of each month at 1300 UK time for 30 mins

Next call: 5th November 2024 *(No call in October)*
1300 UK, 0800 US EST, 2200 Tokyo time

Calls are 30 mins long

We will continue to use Zoom
(Interpretation in Japanese, Chinese and Spanish is available using Zoom's interpretation feature)