PaymentRedesign

TECHNICAL STANDARDS

ASSESSMENT REPORT

7/28/2018

Version 2.0, M. Ficken

1 Table of Contents

VERSION HISTORY

Version	Date	Author	Changes
1.0	7/7/2018	M. Ficken	Initial version for review by ATMIA NextGen committees
2.0	28/7/2018	M. Ficken	Reviewed by ATMIA NextGen Committees

2 Scope

This report will provide an assessment of the relevant collected inventory standards by the ATMIA committee (see Appendix A) with the following results;

1. **Matching Next Gen ATM Blueprint standards with Existing Standards**
   vendor agnostic Infra Standards, App standards, Device Standards

2. **Recommendations on methods for moving forward**
   to develop each of our chosen next gen ATM standards
   to complete the roadmap matrix

2.1 ATMIA Next Gen Blueprint

The NextGenATM blueprint contains three layers;

1) (Host) INFRASTRUCTURE
2) APP SERVICES
3) DEVICES (ATM End Point & Consumer owned)

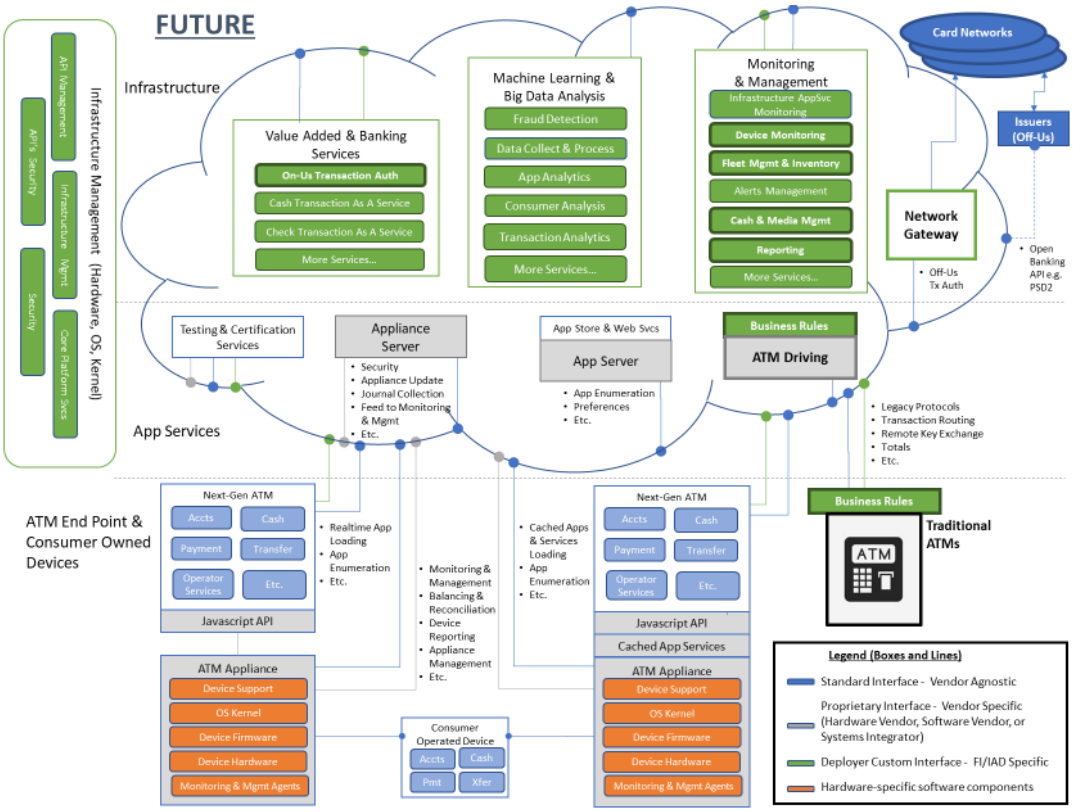


Figure: ATMIA Next Gen Blueprint version 1.1

3 ASSESSMENT

The assessment of the Inventory of Existing Relevant Industry Standards (see appendix A) are by type of standard and assigned to one or multiple Blueprint domain layers (see paragraph 2.1).

The following Standardisation Types are used:
I/F = InterFace standard specification
SW = SoftWare standard
SEC = SECurity standard

No	Standard Name	Standard Type	Device Domain	App Service	Host Infra
1.	ISO 20022 standard	I/F	X	X	X
2.	ATM ISO 20022 (Nexo) message	I/F	X	X	
3.	JavaScript Object Notation (JSON)	SW	X	X	X
4.	PCI security standards	SEC	X	X	X
5.	PCI PIN on glass	SEC	X		
6.	PCI Cloud security	SEC		X	X
7.	CEN/XFS	I/F	X		
8.	ISO 8583	I/F	X	X	X
9.	ADA *	I/F	X		
10.	EMVco Contactless	I/F	X		
11.	EMVco specifications	I/F	X	X	
12.	ISO-7816 Magstripe	I/F	X		
13.	ISO-14443 NFC / Contactless	I/F	X		
14.	Biometric standards	SEC	X		
15.	ASN.1 - ISO/IEC 8824-1	SW	X	X	X
16.	BER-TLV - ISO/IEC 8825-1	SW	X	X	X
17.	Auto-ID and EDI Communication	I/F			X

The Software (SW) type are generic development standards which can be applied during the implementation of the other standards.

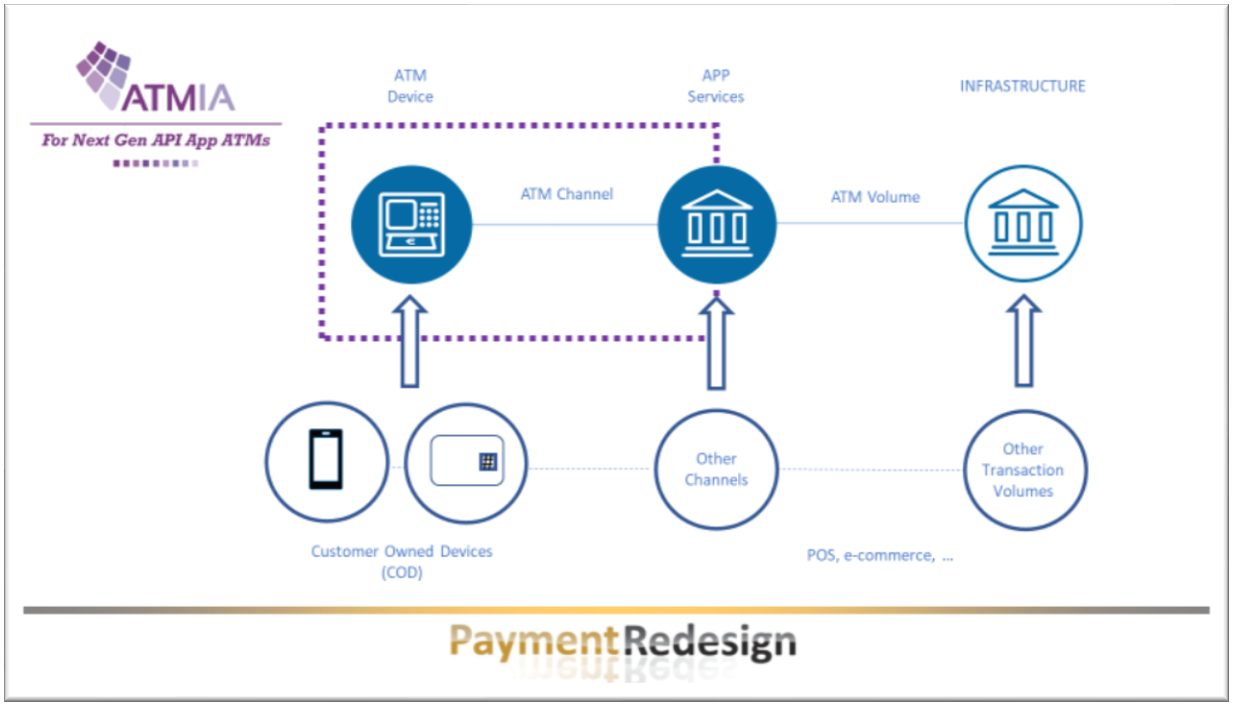
* ADA is an US regional standard, other regional / national standards apply for their geography.

3.1 BIGGER PICTURE

When we place the ATM channel in the bigger picture,
there are other channels and transaction volumes which will have influence too.

Since we are part of a multi-channel environment the APP Services and Host Infrastructure will be used by the Mobile- (COD) & POS channels and transaction volumes too, for the needed scale of economy.

The ATM channel (ATM device and Interfaces to the COD and APP Services) should be the primarily focus for vendor agnostic standardisation, like shown in the figure below.



For example, even the International Card Payment Schemes MasterCard and VISA do not have for the same functionality the same interface specifications, both are ISO8583 based but using a different implementation. The same applies for many domestic interfaces with special domestic functionality.

3.2 Host INFRASTRUCTURE

The trend is for new functionality and interfaces to use the ISO20022 standard as open banking API.

NextGenATM Blueprint Domain	Current Standards	Assessment
Value Added & Banking Services Standard	8 1	ISO8583 mainstream for issuing processing ISO20022 Open banking API, like PSD2
Network Gateway (to cardnetworks) Issuers (off-us)	4	Security PCI-DSS compliant
ATM Machine Learning & Big Data Analysis		
ATM Monitoring & Management Standard	8, 1, 4 17	ISO8583 or ISO 20022 and PCI compliant especially for electronic journal card data. Cash Management, especially for cash replenishment interface

No	Standard Name	Standard Type	Device Domain	App Service	Host Infra
1.	**ISO 20022 standard**	**I/F**	**X**	**X**	**X**
4.	**PCI security standards**	**SEC**	**X**	**X**	**X**
6.	**PCI Cloud security**	**SEC**		**X**	**X**
8.	**ISO 8583**	**I/F**	**X**	**X**	**X**
17.	**Auto-ID and EDI Communication**	**I/F**			**X**

3.3 APP Services

The trend is towards ISO20022 ATM messages, which is created by the Nexo workgroup.

NextGenATM Blueprint Domain	Current Standards	Assessment
Testing & Certification	11 4, (6) 8, (1)	EMVco certification (EMVco testlab) PCI certification (PCI security audit) Card Scheme Certification (MC-MTIP, VISA -ADVT, …)
Appliance Server	4, 6	Security PCI-DSS compliant and PCI-Cloud when used.
App Server	1, 2, 8	ISO8583 legacy, trend new functionality based on ISO20022 open Banking API, especially ISO20022 ATM messages (Nexo)
ATM Driving		

No	Standard Name	Standard Type	Device Domain	App Service	Host Infra
1.	ISO 20022 standard	I/F	X	X	X
2.	ATM ISO 20022 (Nexo) message	I/F	X	X	
4.	PCI security standards	SEC	X	X	X
6.	PCI Cloud security	SEC		X	X
8.	ISO 8583	I/F	X	X	X
11.	EMVco specifications	I/F	X	X	

3.4 DEVICES

The CEN-XFS standard has become mainstream as Multi-Vendor-Software (MVS) API for vendor agnostic hardware. In the NextGen Blueprint we want to make the next step to be O/S agnostic too.

The available CEN-J/XFS standard is O/S & Hardware agnostic and can be made CEN-XFS backwards compatible too. In combination with CEN/XFS4-IoT even ATM Appliance vendor agnostic smart hardware components can be created.

We leverage on the basic technical standards which are required by the Card Schemes (MasterCard, VISA, …) like EMVco (Card and Device) and PCI (Security) including formal approvals.

NextGenATM Blueprint Domain	Current Standards	Assessment
ATM Business Rules	1, 2, 8	ISO8583 legacy, trend new functionality based on ISO20022 open Banking API, especially ISO20022 ATM messages (Nexo)
Next-Gen ATM	4, 5	PCI security compliance
	9	Disability accessibility standard
Javascript API	7	CEN-XFS mainstream (windows O/S), O/S agnostic possible by available J/XFS
ATM Appliance	4, 5	Security PCI compliancy, like PCI-PED
	7	CEN/XFS4-IoT future smart-components
	9	Disability accessibility standard
	10, 13	Contactless ISO-EMVco-NFC I/F standards
	12	Magstripe standard
Cached App Services	13	EMVco approved ATM appliances
	14	Biometric Standards
Consumer Operated Devices	10, 13	Contactless standards (ISO-EMVco-NFC)
	4, 5	PCI security, e.q. PIN of glass
	13	EMVco approval
	14	Biometric Standards, e.q. fingerprint

No	Standard Name	Standard Type	Device Domain	App Service	Host Infra
1.	ISO 20022 standard	I/F	X	X	X
2.	ATM ISO 20022 (Nexo) message	I/F	X	X	
4.	PCI security standards	SEC	X	X	X
5.	PCI PIN on glass	SEC	X		
7.	CEN/XFS	I/F	X		
8.	ISO 8583	I/F	X	X	X
9.	ADA	I/F	X		
10.	EMVco Contactless	I/F	X		
11.	EMVco specifications	I/F	X	X	
12.	ISO-7816 Magstripe	I/F	X		
13.	ISO-14443 NFC / Contactless	I/F	X		
14.	Biometric standards	SEC	X		

4 IMPACT

The table below shows which standards are relevant for which ATMIA NextGen committee.

No	Standard Name	Standard Type	Technical	Customer	Security
1.	ISO 20022 standard	I/F	X		
2.	ATM ISO 20022 (Nexo) message	I/F	X		
3.	JavaScript Object Notation (JSON)	SW	X		
4.	PCI security standards	SEC	X		X
5.	PCI PIN on glass	SEC	X		X
6.	PCI Cloud security	SEC	X		X
7.	CEN/XFS	I/F	X		
8.	ISO 8583	I/F	X		
9.	ADA	I/F	X	X	X
10.	EMVco Contactless	I/F	X		
11.	EMVco specifications	I/F	X	X	X
12.	ISO-7816 Magstripe	I/F	X		
13.	ISO-14443 NFC / Contactless	I/F	X		
14.	Biometric standards	SEC	X	X	X
15.	ASN.1 - ISO/IEC 8824-1	SW	X		
16.	BER-TLV - ISO/IEC 8825-1	SW	X	X	X
17.	Auto-ID and EDI Communication	I/F	X		X

4.1 Technical Committee

Next Gen ATM - Impact of Existing Regulations & Standards on the Blueprint	
Subcommittee: Technical / Customer / Security / ….	
Impact	***Discussion***
Existing Standard is Consistent With the Blueprint	ALL 1-17
Existing Standard Conflicts With the Blueprint	CEN-XFS (not O/S agnostic) ISO8583 between NextGen App and ATM Driver APP Service (should be ISO20022 ATM msg)
Existing Standard Does Not Address the Blueprint, Additional Work or Standard May Be Needed	Expected Additional work needed for full backwards compatibility of J-XFS and XFS4-IoT to current CEN-XFS functionality and to add additional higher level javascript layer too.
It's Unclear Whether the Existing Standard is Sufficiently Aligned With the Blueprint	
Existing Standard is Not Relevant / Mandatory to the Blueprint*	These are generic development standards which can be advised to apply during the implementation of the other standards but are not forced / mandatory to be used to be blueprint compliant. (3) JSON (15) ASN.1 (16) BER-TLV

4.2 Customer Committee

Next Gen ATM - Impact of Existing Regulations & Standards on the Blueprint	
Subcommittee: Customer	
Impact	***Discussion***
Existing Standard is Consistent With the Blueprint	**(9) ADA** **(11) EMVco (user interface)** **(14) Biometric Standards**
Existing Standard Conflicts With the Blueprint	
Existing Standard Does Not Address the Blueprint, Additional Standard May Be Needed	
It's Unclear Whether the Existing Standard is Sufficiently Aligned With the Blueprint	
Existing Standard is Not Relevant to the Blueprint*	

* This assessment should be made from the perspective of each subcommittee's different area of focus. For example, the Security Subcommittee may find a particular regulation or standard to be relevant, but the same regulation or standard may not be relevant to the Customer Interface Subcommittee.

4.3 Security Committee

Next Gen ATM - Impact of Existing Regulations & Standards on the Blueprint	
Subcommittee: Security	
Impact	***Discussion***
Existing Standard is Consistent With the Blueprint	**(4) PCI security standards** **(5) PCI PIN on glass** **(6) PCI Cloud security** **(9) ADA** **(11) EMVco (security standards)** **(14) Biometric Standards**
Existing Standard Conflicts With the Blueprint	
Existing Standard Does Not Address the Blueprint, Additional Standard May Be Needed	
It's Unclear Whether the Existing Standard is Sufficiently Aligned With the Blueprint	
Existing Standard is Not Relevant to the Blueprint*	

* This assessment should be made from the perspective of each subcommittee's different area of focus. For example, the Security Subcommittee may find a particular regulation or standard to be relevant, but the same regulation or standard may not be relevant to the Customer Interface Subcommittee.

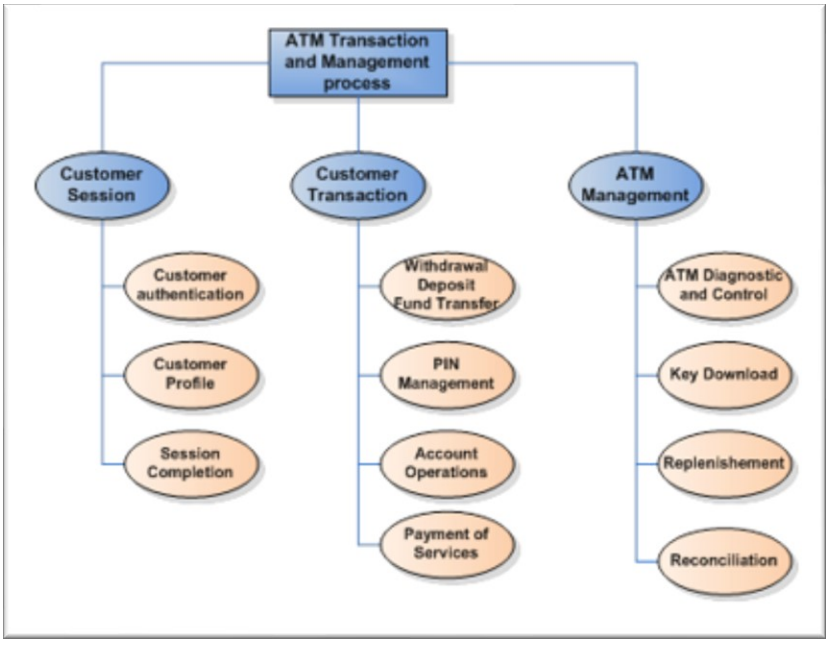
5 RECOMMENDATIONS

Based on the assessment we have the following recommendations.

5.1 NextGen APP functionality

The functionality in the NextGen APP's will be the main driving force and direction of the next steps. Starting with the NextGen APP and transaction flow description of the NextGenATM Blueprint.

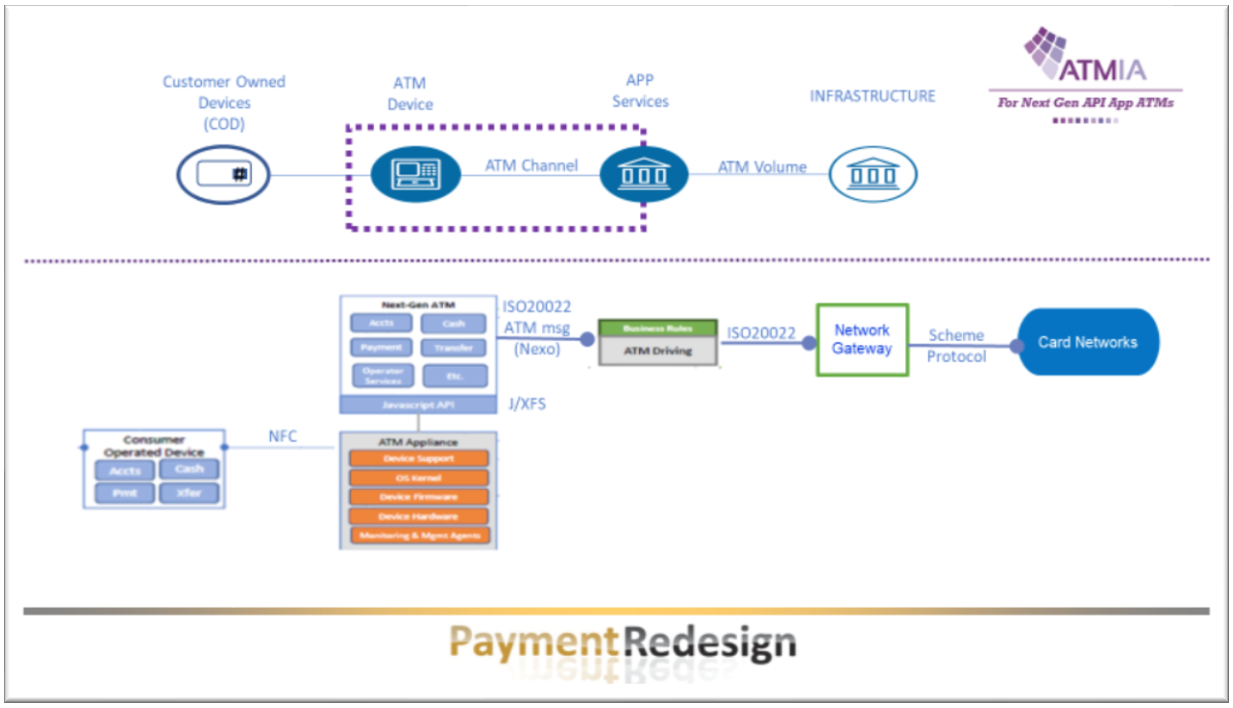
The high-level business processes covered by ISO20022 ATM messages (Nexo) standard would be a good starting point, like shown in the figure below, which functionality should be vendor-agnostic.



Source: ISO20022 ATM message – high level business process

EXAMPLE: Customer Transaction – Withdrawal

The figure below shows the involved ATMIA NextGen Blueprint standards for the vendor agnostic user function “Cash Withdrawal” process flow.



We recommend making the user interface device agnostic or even better the NextGen App, so the same NextGen ATM app can run on the ATM device and the Customer Owned Mobile Device.

5.2 Implementation Model

The implementation model should define the level playing field (competition space) with freedom of development implementation choices and standardisation (co-operation space) which can be validated and certified.

Now the direction of the needed standards for NextGen are clearer,
it is good to discuss the implementation model in the NextGen technical committee.

APP-Model
Will there be an open model look-a-like mobile phones with native apps, hybrid apps, cloud apps and browser apps using thin-client app with a (cloud-based) FAT server and/or a FAT client app with a thin server or will only be one of these app models be allowed?

The JavaScript API (NextGenATMia kernel) and NextGenATM APP should preferably be device agnostic too, so it can run on ATM devices and Customer Owned mobile Devices. (Android and IOS) To create the same common user experience without additional impact, ea. integrate in the mobile banking app of the issuing bank.

To make the vendor agnostic functionality (blue) crystal clear it could be possible to allow non-vendor agnostic apps and functionality (green and orange) in the NextGen ATM APP domain. The non-vendor agnostic API can, when less competitive anymore in the future, be the input to create the future vendor agnostic NextGen API version.

Single / Multi development
Even for some standardisation components it is the question if every vendor should develop this (multiple developed solutions) based on the specifications or
that ATMIA should provide this component as a library (single developed solution) to be integrated in the multiple developed ATM solutions.

For example, should we build one “ATMIA NextGenATM Kernel” Javascript API which can be used by all vendors to be integrated or let every vendor develop this common component.

Certification Service
Which implementation model for certification services will be used
to provides the report with results for ATMIA NextGen approval;

a) certifications by a 3rd party accredited Test Lab (a la EMVco)

b) self-certification by vendor using an ATMIA certification tool (a la Visa, MasterCard)

c) own ATMIA Test Lab service (in each region)

For any of these models to work, a comprehensive functional and technical specification is required as well a complete set of test cases and test plans.

5.3 ATMIA Role

Which role(s) does ATMIA wants to fulfil will be important too.
The collected inventory standards document by the ATMIA committee (Appendix A) stated;

"ATMIA can play a global independent role for developing specifications and certification, similar to the EMVco model, for Next Generation ATMs. This role could, in turn, generate revenues for further development and maintenance of the ATMIA NextGenATM specification and certification service."

Like EMVco the ATMIA brand can become an official NextGen compliance certificate for ATM solutions which follow the NextGen blueprint, standards and passed the certification. The process to get this formal NextGenATMia approval certificate generate revenues.

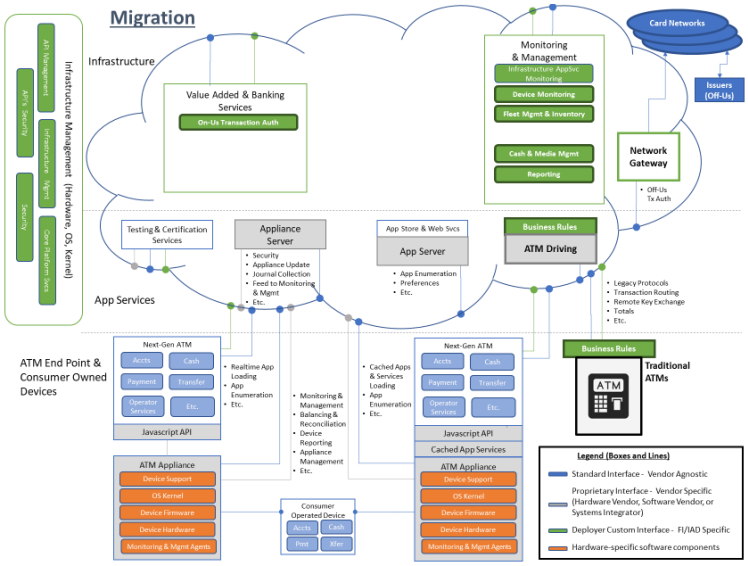
ATM Deployers and Bank create the demand for this NextGenATMia certificate and the ATM vendors can differentiate to show following the NextGenATMia Blueprint latest standards and easy integration with other NextGenATMia solutions.

Recommend ATMIA to plan a governance structure for monitoring and preventing potential fraud, and maintaining long term interoperability too.

5.4 Reference Implementations

We recommend developing some Reference Implementations on multiple Operating Systems (O/S) and operational configurations to;

- validate the blueprint, specifications and flows, they are clear and do not contain gaps
- gain implementation experience to be included in the final version
- demonstrate implementation reference showcases during ATMIA events in 2019



5.5 Roadmap

1. **Define NextGenATMia Implementation Guide 1.0** **Q3-Q4 2018**
   Containing NextGen Blueprint, Technical Standards,
   Vendor Agnostic Functional Flow (see paragraph 5.1) and
   Implementation Model (see paragraph 5.2)

2. **Develop Reference Implementations** (see paragraph 5.4) **Q4–Q1 2019**
   to validate the specifications, gain implementation experience and demonstrate implementation reference showcases for ATMIA events in 2019.

3. **NextGenATMia Implementation Guide version 2.0** **Q1 2019**
   based on validated reference implementations to have the majority of possible NextGen implementation issues tackled (ATMIA US)

APPENDIX A: Inventory of Existing Relevant Industry Standards

1. **ISO 20022 standard** is intended to be a single message standard for all financial communications, irrespective of the counterparty (financial institutions, market infrastructures, corporate customers, and the like), the business domain (payments, securities, treasury, trade services, etc.), or the network (public or proprietary, domestic or international).
2. **ATM ISO 20022 (Nexo) ATM messaging standard** (www.nexo-standards.org/standards/nexo-atm-protocol)
   The Nexo-IFX ATM protocol is the first universal standardisation initiative related to the ATM transaction and management domain.
3. **JavaScript Object Notation (JSON)**
   a. A programming language which is OS-independent that could be suitable for:
      - ATM Client to ATM Host Communication
      - Hardware Device Service Provider to ATM Client Communication
      - Platform Independent (portable) Hardware Abstraction Layer (HAL) to ATM Client Communication
   b. Note: JSON is capable of supporting the Windows Ecosystem on x86-64 and Linux on x86-64 and ARM.
4. **PCI security standards**
   Global, open industry standards for Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS); plus ATM Security Guidelines which address the software, hardware and device components of the ATM.
5. **PCI PIN on glass (PIN-Entry on customer device)**
   https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Updates_Payment_Device_Standard_To_Support_SPoC_9_March.pdf
6. **PCI Cloud security**
   https://www.pcisecuritystandards.org/pdfs/Cloud_SIG_Release.pdf
7. **CEN/XFS**
   CEN/XFS (extensions for financial services) provide a client-server architecture for financial applications on the Microsoft Windows platform, especially peripheral devices such as EFTPOS terminals and ATMs which are unique to the financial industry. They are international standards promoted by the European Committee for Standardization (known by the acronym CEN, hence CEN/XFS). The standard is based on the WOSA Extensions for Financial Services or WOSA/XFS developed by Microsoft. With the move to a more standardized software base, financial institutions have been increasingly interested in the ability to pick and choose the application programs that drive their equipment. CEN/XFS provides a common API for accessing and manipulating various financial services devices regardless of the manufacturer.

All previous versions of the CEN/XFS standard will work only under Windows, however CEN/XFS4-IoT is a major departure from all previous versions in that it is OS Agnostic (i.e. will run on Windows, Linux, Android, etc). In addition, it can run in low resource environment, e.g. embedded and can have end to end application level security.

8. **ISO 8583** is an international standard for financial transaction card originated interchange messaging. It is the International Organization for Standardization standard for systems that exchange electronic transactions initiated by cardholders using payment cards. It is the Transaction Gateway to International Schemes with specific ISO-8583 implementations like MasterCard, Visa, etc.
    a. It defines a message format and a communication flow so that different systems can exchange these transaction requests and responses. The vast majority of transactions made when a customer uses a card to make a payment in a store (EFTPOS) use ISO 8583 at some point in the communication chain, as do transactions made at ATMs. In particular, both the MasterCard and Visa networks base their authorization communications on the ISO 8583 standard, as do many other institutions and networks. Although ISO 8583 defines a common standard, it is not typically used directly by systems or networks. It defines many standard fields (data elements) which remain the same in all systems or networks, and leaves a few additional fields for passing network-specific details. These fields are used by each network to adapt the standard for its own use with custom fields and custom usages.
9. **ADA** (and similar regulations in other countries) - The Department of Justice's revised regulations for Titles II and III of the Americans with Disabilities Act of 1990 (ADA) were published in the Federal Register on September 15, 2010. These regulations adopted revised, enforceable accessibility standards called the 2010 ADA Standards for Accessible Design, "2010 Standards." https://www.ada.gov/2010ADAstandards_index.htm
10. **EMV Contactless** https://www.emvco.com/emv-technologies/contactless/
    a. Contactless cards or NFC based mobile phones use standards like EMV contactless even if the physical card is represented through a virtual card.
11. **EMVco specifications** (hardware, kernel, application) + certification specs
12. **ISO-7816 Magstripe**
13. **ISO-14443 NFC / Contactless**
14. **International and national biometric standards**

15. **ASN.1 notations - ITU-T X.680 | ISO/IEC 8824-1**
    (Abstract Syntax Notation One - ASN.1)
    a. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12479&lang=en
    b. Defining rules for data exchange that are vendor agnostic, even if the contents could be vendor specific in some cases; could be useful for defining the formats for data exchange along all the interfaces, even those that carry proprietary data, in a way that any system could be able to interpret, even in cases where part of the content would not be relevant for that particular system, sub-system or module.
16. **BER-TLV - ITU-T X.690 | ISO/IEC 8825-1 (Basic Encoding Rules - BER and others)**
    a. https://www.itu.int/ITU-T/recommendations/rec.aspx?id=12483&lang=en
    b. Defining rules for data exchange that are vendor agnostic, even if the contents could be vendor specific in some cases; could be useful for defining the formats for data exchange along all the interfaces, even those that carry proprietary data, in a way that any system could be able to interpret, even in cases where part of the content would not be relevant for that particular system, sub-system or module.
17. **Auto-ID and EDI Communication standards** for all cash replenishment processes and inventory data transfers. Electronic data interchange (EDI) is the concept of businesses electronically communicating information, such as for purchase orders and invoices.

Roadmap for Proposed Next Gen ATM Industry Standards

Name of Standard	Location in Next Gen Architecture	Type of Standard	Recommend Method for Developing Standard
Testing & Certification Standard	App services	EMVco Model	
Value Added & Banking Services Standard	Infrastructure	ISO20022	
A Standard for ATM Machine Learning & Big Data Analysis	Infrastructure	t.b.d.	
ATM Monitoring & Management Standard	Infrastructure	ISO20022	
Open Banking API Standard (e.g. PSD2)	Network Gateway	ISO20022	
Network Gateway Standard	Network Gateway	ISO20022	
Standard for Business Rules at ATM	App Services & ATM End Point	UML or other Business Rule Mngt System.	
ATM Driving Standards	App Services	ISO20022 ATM msg (Nexo)	
Cached App Services Standard	App Services & ATM End Point	FAT client implementation model dependent	
Javascript API	App Services & ATM End Point	CEN/J-XFS	NextGenATMia Kernel ?
App Server Standard	App Services	Implementation Model dependent	
ATM Appliance Standard	App Services & ATM End Point	Implementation Model dependent	
Appliance Server Standard	App Services	Implementation Model dependent	
Customer Owned Device Interface Standard	Customer Owned Device	Card Scheme dependent (EMVco specs)	

ATMIA can play a global independent role for developing specifications and certification, similar to the EMVco model, for Next Generation ATMs. This role could, in turn, generate revenues for further development and maintenance of the ATMIA NextGenATM specification and certification service.