



**ASC X9, Inc.**  
**NEW PROJECT PROPOSAL FORM**

**1. TYPE OF PROJECT – PLEASE CHECK ONE**

- X NEW PROJECT FOR NEW ANS/TR/DSTU
- NEW PROJECT ADOPTION OF ISO STANDARD  
(PER X9 PROCEDURES, REQUIRES BOARD APPROVAL)
- REVISION PROJECT FOR ANS/TR  
(PER X9 PROCEDURES DOES NOT REQUIRE BOARD APPROVAL)
- INTERNAL EXTENSION OF PROJECT TIMELINE SET BY BOARD  
(REQUIRES BOARD BALLOT AND SHALL INCLUDE REASON FOR EXTENSION)
- EXTERNAL EXTENSION OF ANS PERIODICAL REVIEW

**2. INFORMATION ABOUT PROJECT AND PROPOSER**

Project Title: *Protection of Sensitive Card Data between Device and Acquiring System*

Date of Submittal: *DRAFT 1*

Name of Proposer: *Sid Sidner*

Organization: *ACI Worldwide*

**3. JUSTIFICATION OF PROJECT**

**a.) Issue Description:** *(Provide a detailed explanation of what you propose to standardize. Attach any documents to further explain subject.) Attach draft if available.*

*Theft of sensitive card data during a retail payment transaction is increasingly becoming a major source of financial fraud. Besides an optional encrypted PIN, this data includes magnetic stripe track 2 data: PAN, expiration date, card verification value, and issuer private data. While thefts of this data at all segments of the transaction processing system have been reported, the most vulnerable segments are between the point of transaction device capturing the magnetic stripe data and the processing systems at the acquirer.*

*This document would standardize the security requirements and implementation for a method for protecting this sensitive card data over these segments. Several implementations exist to*

*address this situation. This document would provide guidance for evaluating these implementations.*

*This work needs to consider the typical topology of these segments, including device, store controller, merchant host system, processor system, and the acquirer's systems and networks. The definition of how far up the transaction path this standard should apply is important. It also needs to consider the processing, including payment authorization and settlement, returns, and gift cards, for example.*

*Several key differences exist between this document and the documents regarding PIN security:*

- *PINs must never be in the clear except inside a TRSM (Tamper Resistant Security Module). However, the sensitive card data is often in the clear in the processing nodes between the segments.*
- *Exposure of this data does not carry the risk associated with exposure of PINs.*
- *Encryption/decryption might be able to be done in software for performance reasons. This implies the following*
  - o *Encryption keys in cleartext.*
  - o *The data cleartext and ciphertext may be available in the same memory space.*

**b.) Project Need/Benefit:** *(Please include a thorough explanation of why the standard is needed, what commercial, operational, or financial benefits may be realized by use of the standard.)*

*Merchants are incurring extraordinary costs in trying to protect this data. A method that protected the data at the device might allow merchants, processors, and acquirers to realize dramatic cost savings with implementation of this standard.*

*This work would provide a way to evaluate existing implementations and as a guide to new implementations.*

**c.) Identify Stakeholders:**

*Merchants*

*Processors*

*Acquirers*

*Hardware & Software Providers to these Stakeholders*

*Issuers & Payment Brands (because it protects their card data)*

**d.) Is this project a consumer product?**

*No.*

**f.) Does it contain any units of measurement?**

*No.*

**If yes, which one:**

- U.S.**
- Metric**
- Both**
- Not Applicable**

#### **4. COORDINATION WITH OTHER STANDARDS**

a.) Do you see this as a technical report (TR) or a standard (ANS)?  
(Refer to X9 Procedures for explanation.)

*This would be could either be an ANS and a TR, an ANS with an annex describing an implementation, or a TR with initial sections that specify requirements.*

b.) Could this technical report/standard become part of another X9 technical report/standard?

*Some people have proposed that this could be a part of X9.114. However, the work to date on X9.114 attempts to address the total operational protection of financial data processing, including hardware and software security, as well as operational and personnel security. This new standard would be focused exactly on the protection of data between the merchant and the acquirer.*

c.) Should this project be developed within ISO/TC68 as an international standard?

*Like other X9 standards regarding card security, this could be proposed to ISO/TC68 for incorporation into an ISO standard.*

d.) List any closely related domestic standards either published or under development of which you are aware.

*ANS X9.8*

*ANS X9.24*

*ANS X9.114*

*Payment Card Industry Data Security Standard (PCI DSS)*

*Payment Card Industry Payment Application – Data Security Standard (PCI PA-DSS)*

e.) Describe any related domestic work efforts.

*Payment Card Industry Security Standards Council (PCI SSC)*

f.) List any closely related international standards, either published or under development of which you are aware.

*None.*

g.) Identify the ISO standard or technical report to be adopted.

*N/A.*

h.) Does this project contain text from an ISO standard?

No.

i.) Security-related Needs:

(Identify any security-related needs or requirements generated by this new work item and discuss them with the chair of the X9F Data & Information Security subcommittee. Will any of these needs or requirements be included in the scope statement?)

*Yes, I would expect these to be included in the scope statement.*

*Cryptographic protection of the data will likely be employed. If symmetric cryptography is used, for example, the current PIN security standard supports three types of protection keys: PIN, MAC, Data. The Data key could possibly be used. However, care needs to be taken the data may be available in both cleartext and ciphertext outside a TRSM needs to be considered. Also, the cryptography may most practically be performed in software, with or without the keys protected using methods that require a TRSM. The risks associated with this need to be considered.*

**5. PATENT ISSUES AND GOOD FAITH DEVELOPMENT PRACTICE**

Any party who proposes or becomes aware of an item, which is patented or intended for patent, for inclusion in a standard or guideline under development, shall immediately inform the working group that the item is covered by a patent. This requirement holds whether or not the party proposing the item is the holder of the patent.

Are there any patent concerns or could there be in conjunction with this project?

*None are held by the proposing party, nor is the proposing party aware of any other applicable patents.*

**6. PROJECT TIMELINE AND PARTICIPATION (A and B)**

Estimated Project Development Time  
(See X9 timelines requirements below)

Note that X9 requires:

Status ////////////////////////////////////	Definition //////////////////////////////////////	Timeline //////////////////////////////////////	
New Work Item (NWI) Revision	New standards development project or revision	Approval of NWI by Board is the NWI project start date – sets to 0 Revisions timelines start with notification to the Board – sets date to 0	T0
Working Draft (WD)	A working draft is created by the working group	A draft of the new standard or revision is due between, but no later than 18 months 0-18 months	T0 + 6 months
Committee Draft (CD)	A draft has been issued to be balloted to the Subcommittee	For either a new work or revision, at 18 months ballot to SC should have begun	T0 + 12 months

Draft Industry Standard	The document has been issued to be balloted to the Consensus body – X9	For either a new work or revision, the document should be balloted no later than 18-36 months	<i>T0 + 24 months</i>
Published	Completed and available for sale	For either a new work or a revision, the document should be published no later than 36-40 months	<i>T0 + 30 months</i>
Periodical Review		5 year review due from date of ANSI approval	<i>T0 + 90 months</i>

**Potential participants :** *(List names and organizations - Must include at least 5 X9 Board voting organizations)*

*ACI Worldwide  
Delap LLP  
Dresser Wayne  
Gilbarco  
HP Atalla  
Hypercom  
IBM  
Ingenico  
Key Innovations  
Merchant Advisory Group*

**7. MARKETING INFORMATION**

What is the target audience for this guideline or standard?

*POS Device Implementers  
ATM Implementers  
Store Controller Implementers  
Retail Host System Implementers  
Processing System Implementers  
Acquiring System Implementers*

What industry need will the standard or guideline fill and how?

*Protection of payment card transaction data at merchants and processors.*

How will X9 "sell" the standard or promulgate its use?

*This will may make PCI DSS compliance much easier by merchants and processors.*

**8. RETURN COMPLETED FORM TO:**

Cindy Fuller, ASC X9, Inc.  
1212 West Street, Suite 200  
Annapolis, Maryland 21401

Telephone: (410) 267-7707  
Fax: (410) 267-0961  
Email: admin@X9.org

One