HSM Evolution in Automotive: Opportunities of Standardization

Raymond Li

Uni-Sentry

伊世智能
UNI-SENTRY

1. **Background**
2. Key Challenge
   and Opportunities of Standardization
3. Case Study

01-Compliance

伊世智能 UNI-SENTRY

- **Mandatory** **Vehicle Regulations and Standards (R155 and GB-44495) Compliance with Process and Product Security.**

Resource: Global Platform 2025

02-HSM Recommended

- **HSM(Hardware Security Module)is recommended to use as "Trust Root" by Regulations and Standards for supporting Secure boot, Secure Communication...**

Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
20.1	Illegal/unauthorised changes to vehicle's electronic ID	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP

8.3.5 数据安全测试

8.3.5.1 密钥防非法获取和访问安全测试

测试人员应依据车辆密码使用方案，确认测试零部件，并按照以下三种测试方法中适用的测试方法开展测试，判定车辆是否满足 7.4.1 的要求：

a) 若采取安全访问技术存储密钥，通过零部件访问接口进行破解、提取等攻击操作，测试是否可对密钥非授权访问和获取；

b) 若采取 HSM 等硬件安全模块存储密钥，应依据硬件安全模块安装位置说明文档，检查车辆是否在文档标识位置安装了硬件安全模块来保护密钥；

c) 若采取安全的软件存储形式存储密钥，应依据车辆制造商提供的保证车辆密钥安全存储证明文件，检查是否安全存储密钥。

Resource: R155 Annex 5 and GB 44495

03-Milestone

Automotive HSM Standards/References Development Milestones

- **EVITA**

  2008 : EU launched the EVITA project (continued until 2011)

  2011 : Released three-tier HSM architecture (Full/Medium/Light)

- **SAE J3101**

  2016 : SAE&GP first published hardware security standard

  2020 : Incorporated into AUTOSAR reference architecture

- **SHE/SHE++**

  2016 : Audi/BMW jointly released initial specification

  2020 : Upgraded to support AES-256 and ECC-256 algorithms

04-Relationship

Standard	Secure Level	Capability	TOE	HW Protection
EVITA	Full/Medium /Light	-Asymmetric Encryption（RSA/ECC） -Secure Communication（TLS/SecOC） -Physical Attack Resistance (Side-Channel) -AES-128 Symmetric Encryption -Basic Key Management -Secure Boot -AES-128-CMAC -Secure Boot	- GW、V2X等 - In Vehicle Communication (CAN/Ethernet) -Sensor、Actuators ECUs	-MCU(HSM) -Logical Isolation
SAE J3101	Level1-4+	- Advanced Physical Attack Resistance（Laser Fault Injection） Common Criteria EAL4+ -Basic Physical Attacks（Probing、Voltage Glitching） -SW Tamper Resistance -Secure Boot -Basic Crypto. Operations（No HW）	-High-Safety Domain （ADCU） -Medium & Safety-Critical ECU（EPS） -Low-Safety ECU	-Certified Lab-Grade Protection -Physical Tamper Resistance (Anti-Disassembly) -Logical Protection (Memory Encryption)
SHE/SHE++	SHE/SHE++	-AES-256/ECC-256 -Dynamic Key Management -Enhanced Secure Boot -AES-128 -Fixed Key Hierarchy（Master/Slot）	-Single-ECU (Engine Control Unit Security)	-EVITA Medium -EVITA Light

Note: The depth of color is related to the level of secure importance.

05-Relationship

Summary

1. EVITA standard focuses on functional and performance classification, covering full-scenario requirements from complex domain/ECUs (gateways) to simple sensors.
    - Complex gateways： TLS 1.3 with ECDSA-384 support （EVITA Full)
    - Simple sensors： AES-128-CMAC only （EVITA Light)
2. SAE J3101 emphasizes hardware attack resistance, applicable to cross-domain security certification。
    - Hardware Attack Resistance: Must pass the following tests:
        - Side-Channel Attack (SCA) Testing: ISO 17825
        - Fault Injection Attack Testing: IEC 62443-4-2
    - Vehicle Side： AutoSAR Secure Hardware Extensions
      Cloud： FIPS 140-3 Level 3
3. SHE/SHE++ specifications target algorithm and key management optimization for individual ECUs.

伊世智能
UNI-SENTRY

1. Background
2. **Key Challenge and Opportunities of Standardization**
3. Case Study

0201-Key Challenge

Regional Compliance Variations

1. EU/China (Partial)：EVITA+SHE++ (German Supply Chain Dominant)
2. North America/China (Partial)：SAE J3101 (US Supply Chain Dominant)

Key Management Compatibility Issues

1. AES-128/256、SHA-256 Compatible，but KM(SHE&EVITA) and Asymmetric (SAE J3101 no ECC)
2. SM Series，and PQC not yet supported

Dimension	EVITA	SAE J3101	SHE++
Regional	EU/China（GB/T）	North America/China	German、EU
PQC (Kyber/Dilithium)	Evaluation	Not Yet（Level 4+Extension)	No
SM（2、3、4)	No	No	No

0201-Opportunity

伊世智能 UNI-SENTRY

- Regroup and Matching:
  - High-Safety Domain： EVITA Full + SAE Level 4+ + SHE++ (ECC-256)
  - In Vehicle Communication: EVITA Medium + SAE Level 3+SHE++（Partial）
  - Low-Safety ECU: EVITA Light+ SAE Level 2+SHE

Secure Level	EVITA	J3101	SHE	TOE	Capability
High	Full	Level 4+	SHE++	-GW、ADAS、 V2X..	- ECC-256/AES-256 - Physical Attack Resistance - Dynamic Key Management
Medium	Medium	Level 3	SHE++	- In Vehicle Communication (CAN/Ethernet)	- AES-128/256 - Secure Boot - Probing Attack Resisitance
Low	Light	Level 1-2	SHE	- BCM.. (Window..)	- AES-128-CMAC - Fix Key Management - SW Tamper Resistance

Note: The depth of color is related to the level of secure importance.

0201-Opportunity

Key management Integration

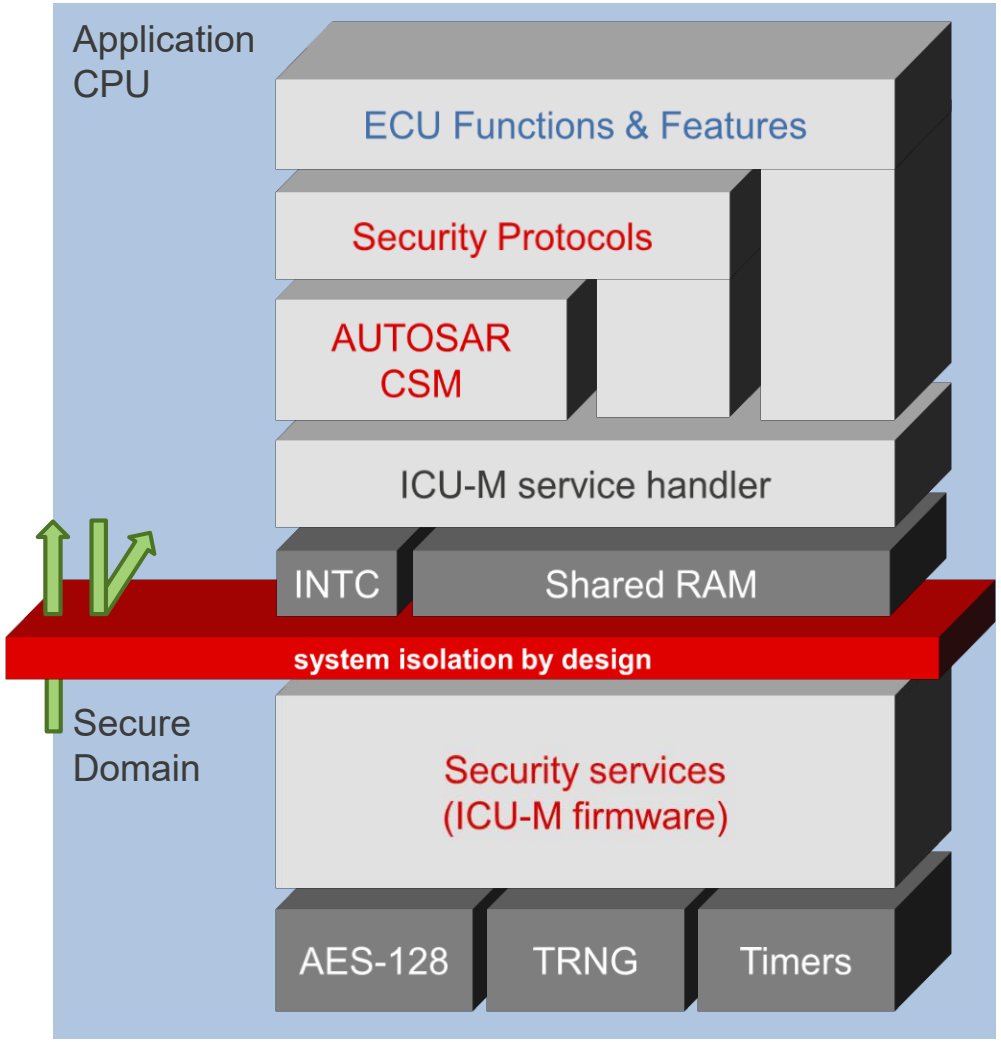
1. EVITA Medium (2011) partially interoperates with SHE++ v1 (2016) in key management.
2. The Crypto Abstraction Layer (CAL) abstracts low-level discrepancies, facilitating cross-standard coordination via AUTOSAR or **HSM firmware**.

Scenario	Key Challenge	Opportunity
EVITA Full <->SAE L4	The static key slots in SHE are inherently incompatible with EVITA's dynamic key derivation mechanism	AutoSar Crypto Stack
SAE Level 3 <-> SHE++	The hardware-bound key scheme in SAE is incompatible with SHE++'s dynamic key derivation approach	HSM Firmware

0201-Opportunity

Standard API Integration

1. HSM firmware must interact with the AUTOSAR BSW layer through standardized interfaces to ensure compatibility in key management and cryptographic operations.
2. The **MCAL layer** must provide **HSM hardware drivers** supporting register-level operations for mainstream security chips (e.g., **Infineon**, **Renesas**)



Resource: RH850 handbook

0202-Key Challenge and Opportuinty

伊世智能 UNI-SENTRY

How to test?

- **Physical Protection** (Key Storage Isolation, Anti-Tampering)
- **Side-Channel Attack Resistance** (Power Analysis, Timing Attacks)
- **Code Scanning**

....

Which part get security evaluation certification?

- **FW Integrity** (Vulnerability Scan..)
- **Algo**.(SM/AES…)
- **Physical Protection**(SCA…)

....

How to test

- Hardware-level isolation (e.g. HSM or Secure Enclave)
- Tamper-proof design (e.g. epoxy resin encapsulation, photosensitive self-destruction circuit)
- Testing standard: ISO 17825 (Side-channel attack test methodology)
- Compliance check (e.g. MISRA C/C++, AUTOSAR C++14)

。。。

Where to get security evaluation certification

- CATARC/CC EAL4+
- CAVP-NIST/OSCCA
- FIPS 140-2/3…

伊世智能
UNI-SENTRY

1. Background
2. Key Challenge
   and Opportunities of Standardization
3. **Case Study**

伊世智能
UNI-SENTRY

1. Background
2. Key Challenge
   and Opportunities of Standardization
3. **Case Study （HSM FW）**

0301-HSM FW General Requirements

伊世智能 UNI-SENTRY

	ICU-M Firmware Service	ICU-M Firmware Service Summary
1	Encryption / decryption	AES(128bit key), RSA(~3072bit key) encryption/decryption
2	CMAC generation / verification	Generate AES-CMAC and verify it
3	RSA signature verification	Signature verification using public key cryptographic method
4	TLS protocol communication	Provide communication functions correspondent to TLS protocol (RFC5246/4492)
5	Hashing	Generate hash for specified data (SHA-1, SHA2, RIPEMD etc.)
6	Random number generation	Generate pseudo random number (AIS-20, NIST SP800-90A algorithm)
7	Key management	Provide key (AES/RSA/ECC key) management (Generation of key or key pair, registration and exportation) services.
8	Monotonic counter management	Irreversible 64 bit-width counter stored in security data flash or RAM
9	Secure boot (Memory cluster verification)	Check the program tampering. Can be executed at boot time or at arbitrary timing.
10	User Code / Data Flash programming services	Flash Programming can be executed securely by ICU-M.
11	Debug access management	Provide 128bit random number challenge & response authentication for debugger connection.
12	Life Cycle management	Available services are restricted based on operating stage (Life Cycle).
13	Customer Expansion Service (CISM)	ICU-M firmware has a mechanism that allows customer to develop additional services

0302-HSM Functional Feature Classic Requirements

伊世智能 UNI-SENTRY

- Secure Boot
  - 安全启动性能优化
  - 安全启动流程设计
  - 安全启动算法
  - 安全启动密钥管理
  - 密钥派生：一机一密；一车一密
  - 密钥更新
  - 错误类型
  - MAC存储
- Secure Storage
  - 安全参数存储接口
  - 安全存储密钥
  - MAC值存储
- KMS
  - 上位机密钥生成
  - 产线密钥注入
  - 密钥更新管理
- Secure Logging
- Secure OTA
  - 验签算法
  - 应用MAC值更新
  - 散列函数及解签算法
  - 断电哈希
  - 层级验签
  - 刷写验签失败安全日志
  - 升级包上位机签名工具
- Secure Debug
  - 27服务
  - 29服务
  - JTAG临时解保护
  - 硬件随机数生成、伪随机数生成器
- Secure Communication
  - SecOC
  - TLS密码套件
  - X.509证书、CVC证书

0303-HSM Crypto Algo. General Requirements

伊世智能 UNI-SENTRY

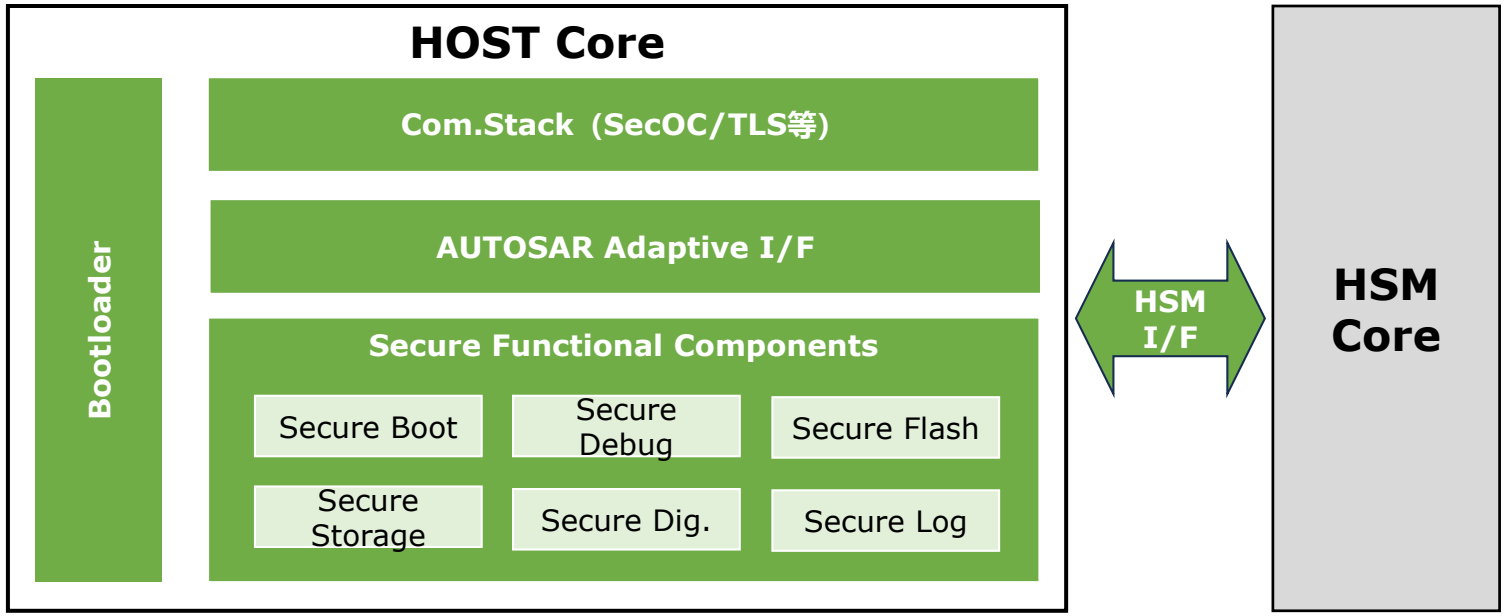
- **TRNG**
  - TRNG/PRNG
- **Internation Algorithm Lib.**
  - Symmetric
    - AES-ECB, CBC, CTR, OFB, CFB, GCM, XTS
  - Asymmetric
    - RSASSA-PSS/RSASSA-PKCS1_v1.5
    - ECDSA (SECP256r1, SECP384r1, SECP521r1)
    - EdDSA (Ed25519ph)
    - RSA (up to 4096)
    - ECC (up to 521)
  - Hash
    - SHA-1
    - SHA-2 (224, 256, 384, 512)
    - SHA-3 (224, 256, 384, 512)
    - SHAKE (128, 256)
  - MAC
    - AEC-CMAC
    - HMAC
- **China Algorithm Lib**
  - SM2
  - SM3
  - SM4
  - SM9
- **PQC**
  - SPHINCS+
  - LMS
  - XMSS
  - FALCON
  - CRYSTALS-KYBER
  - CRYSTALS-Dilithium
- **Key Derivation/Agreement**
  - ECDH/ECDHE
  - KDF
- Cert. Parsing
  - X.509
  - CVC

0304-Supported MCU

IFX	TI	RS	NXP	ST	Native MCU
Aurix TC23XX	AM 261X	RH850 P1H-C	S32K1XX	SPC58N Bernina	国芯CCFC30XX
Aurix TC27XX	AM 263X	RH850 P1H-CE	S32K3XX	Chorus 4M	芯驰E3
Aurix TC29XX	AM 263PX	RH850 P1M-C	S32G	Chorus 6M	地平线J6（alpha）
Aurix TC33XX	AM 623X	RH850 F1KM-S2	MPC5748	Chorus 10M	加特兰ALPS
Aurix TC35XX	AM 62P5X	RH850 F1KM-S4	MPC5561	Stellar (alpha)	杰发AC7840X
Aurix TC36XX	AWR 294x	RH850 U2A8	MPC565		旗芯微FC7300
Aurix TC37XX	TDA4	RH850 U2A12			
Aurix TC38XX	DRA 82X	RH850 U2A16			
Aurix TC39XX		RH850 U2B10			
Aurix TC4XX (alpha)					
Traveo II CYT2B7/9/L					
Traveo II CYT4BF					

0304-Delivery

- E.g.: IFX、RS、TI MCUs based:
  - Secure Application Component: Secure Functional Components (Secure boot..)
  - HSM I/F: Base Layer Interface 和AUTOSAR Crypto-Driver I/F support
  - HSM FW: Crypto Lib and HW Accelerate Engine。。



0308-Test and Certification

- Test Report
- HSM FW Certification

1. HSM 基础功能测试

1. 密钥管理测试

测试人	吴佳斌
测试内容	密钥槽管理。
修复建议	无。
测试步骤	1.调用 SecICHsmBIL_KeyElementSet 对密钥注入，KeyFlag 为默认。 2.调用 SecICHsmBIL_KeyElementGet 读取密钥。 3.调用 SecICHsmBIL_KeyHashGen 获取密钥的 Hash 值比较是否正确。 4.调用 SecICHsmBIL_KeySetValid 设置密钥有效，调用 SecICHsmBIL_KeyGetStatus 获取密钥状态。
期望结果	返回值 HSM_ERC_NO_ERROR，密钥设置有效。密钥的 Hash 值正确。
测试结果	密钥槽管理测试通过。
测试结论	通过。
测试记录	

2. 版本号获取

测试人	吴佳斌
测试内容	版本号获取。
修复建议	无。
测试步骤	1.调用 SecICHsmBIL_GetVersionInfor， SecICHsmBIL_GetHostVersionInfor 获取版本号。
期望结果	返回值 HSM_ERC_NO_ERROR。
测试结果	版本号获取通过。
测试结论	通过。

Functional Test

Files	Active Diagnostics	Violated Rules	Violation Count	Compliance Index
Crypto_SecICHsm_Certificate.c	38	7	85	96.26%
Crypto_SecICHsm_Cipher.c	61	8	150	95.72%
Crypto_SecICHsm_Hash.c	23	7	52	96.26%
Crypto_SecICHsm_Job.c	139	12	288	93.58%
Crypto_SecICHsm_JobQueue.c	52	7	113	96.26%
Crypto_SecICHsm_KM.c	238	8	506	95.72%
Crypto_SecICHsm_Rng.c	14	7	34	96.26%
Crypto_SecICHsm_Signature.c	31	5	86	97.33%
SecICHsmBIL_Certificate.c	92	4	184	97.86%

file:///C/Users/10604/Desktop/[DiAS-EPB] QAC报告/Host_DiAS_EPB_Host_V0.8.6_CWE.html[2024/10/18 18:04:08]

Helix QAC Rule Compliance Report

SecICHsmBIL_Cipher.c	336	8	700	95.72%
SecICHsmBIL_Cmac.c	474	5	951	97.33%
SecICHsmBIL_Hash.c	174	5	350	97.33%
SecICHsmBIL_KeyExchange.c	176	4	352	97.86%
SecICHsmBIL_KeyManagement.c	408	6	822	96.79%
SecICHsmBIL_Random.c	115	4	230	97.86%
SecICHsmBIL_Secuboot.c	116	5	233	97.33%
SecICHsmBIL_Signature.c	108	7	225	96.26%

Vul. Scan Report

CATARC

产品认证证书

PRODUCT CERTIFICATION CERTIFICATE

车载可信安全模块

证书编号/Certificate No. 2024CAC181730139 版本/Version：B0

认证委托人名称及地址 Applicant Name & Address：上海伊世智能科技有限公司/ 中国（上海）自由贸易试验区临港新片区环湖西二路888号C楼 Shanghai Uni-Sentry Intelligent Technology Co., LTD /Building C, No.888 West 2nd Ring Road, Pudong District, Shanghai

商标/Trademark

生产者名称及地址 Producer Name & Address：上海伊世智能科技有限公司/中国（上海）自由贸易试验区临港新片区环湖西二路888号C楼 Shanghai Uni-Sentry Intelligent Technology Co., LTD /Building C, No.888 West 2nd Ring Road, Pudong District, Shanghai

生产企业名称及地址 Factory Name & Address：上海伊世智能科技有限公司/上海市徐汇区桂平路418号6层603号（漕河泾国际孵化中心） Shanghai Uni-Sentry Intelligent Technology Co., LTD/Unit 603, No.418 Guiping Road, Xuhui District, 200233, Shanghai

产品名称及型号 Product Name & Model：车载HSM密码模块 V1.0

产品标准和技术要求 Product Standards & Technical Requirements：CTS CAC-PV18-173：2024

认证模式 Certification Mode：型式试验 Type test

认证结论 Conclusion：上述产品符合CAC-PV18-173：2024《CATARC标志认证实施规则-车载可信安全模块》的要求，特发此证。This is to certify that the above mentioned products have met the requirements of implementation rule CAC-PV18-173：2024

首次发证日期：2024年10月11日 Date of original certification: OCT-11-24　本次发证日期：2024年10月11日 Date of issue: OCT-11-24　有效期至：2025年10月10日 Date of expiry: OCT-10-25

总经理：General manager

中汽研华诚认证（天津）有限公司 CATARC Huacheng Certification (Tianjin) Co.,Ltd

中国·天津·东丽区先锋东路68号科研楼336 300300 NO.68, EAST XIANFENG ROAD, DONGLI DISTRICT, TIANJIN, 300300, P.R.CHINA

CATARC Certification

伊世智能
UNI-SENTRY

THANK YOU

聚焦行业痛点　赋能内生安全