Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Diagnóstico da Situação Atual: eID´s e pesquisa de tecnologias

Data de Emissão:

30/06/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

UNIVERSIDADE DE BRASÍLIA

José Eduardo Cardozo
Ministro

Ivan Marques Toledo Camargo
Reitor

Marivaldo de Castro Pereira
Secretário Executivo

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA

Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA

Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
31/07/2014	0.1	Versão inicial do RT Diagnóstico sobre eID´s e pesquisa de tecnologias- Diagnóstico sobre eID´s.
15/08/2014	0.2	Levantamento de normas e padrões técnicos. - Levantamento dos grupos de pesquisa na área
18/09/2014	0.3	- Levantamento dos estudos e projetos na área. - Levantamento de provedores de soluções, hardware e software para Ids
22/10/2014	0.4	Estudo preliminar de diferentes modelos de identidades nacionais de países da América Latina (Peru, Chile e México), EUA (PIV, TWIC, Real ID), Europa
26/11/2014	0.5	Estudo preliminar de padrões, como o Cartão do Cidadão Europeu (ECC).
11/03/2015	0.6	Estudo de modelos de tecnologias, gerenciamento de tecnologias e emprego em eID's
20/05/2015	0.7	Revisão bibliográfica
30/06/2015	0.8	Versão final

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1 INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Projeto RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Projeto RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, os quais agregam valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto

que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de Identidade Civil – RIC no Brasil.

Este documento é o produto de uma pesquisa inicial sobre padrões, modelos e tecnologias referentes a eID´s, tomando como base todas as atividades previstas na Estrutura Analítica do Projeto de Suporte Tecnológico.

O objetivo deste documento, que não consiste numa pesquisa exaustiva, é fornecer informações, referências de pesquisa e até mesmo orientações e recomendações para os trabalhos subsequentes de pesquisas de tecnologias que subsidiarão o trabalho final de especificação tecnológica, bem como servir como fonte de informação para tomada de decisão junto ao Comitê Gestor.

O relatório é dividido em duas partes. A primeira parte fornece referências sobre normatização, grupos de pesquisa, projetos e infraestrutura para produção de eID´s com o objetivo de servir como guia rápido para pesquisa de informações. A segunda parte engloba um estudo sobre diversos tópicos referentes à emissão, à produção, aos modelos de gerenciamento, tecnologias, e emprego de eID´s, assim como são feitas algumas recomendações úteis para a especificação das tecnologias.

2 NORMATIZAÇÃO, GRUPOS DE PESQUISA, PROJETOS E INFRAESTRUTURA PARA PRODUÇÃO DE eID´S.

2.1 Normatização

Com o objetivo de orientar o trabalho de escolha e adaptação de especificações ao RIC, foi realizada uma pesquisa sobre as principais entidades internacionais de normatização com especificações técnicas pertinentes a tecnologias de *smartcard* [1], RFID [2], modelos de identidade eletrônicas, gerenciamento de identidade [3], protocolos de autenticação e segurança da informação, as quais são listadas com uma descrição sucinta, a saber.

a. Organização Internacional para padronização/ Comissão Internacional Eletrotécnica (*International Organization for Standardization/ (International Electrotechnical Commission*- ISO/IEC):

Norma	Descrição
ISO/IEC 7816	*Identification cards - Integrated circuit cards*
ISO/IEC 7810	*Identification cards - Physical characteristics*
ISO/IEC 7811	*Identification cards - Recording technique*
ISO/IEC 7812	*Identification cards - Identification of issuers*
ISO/IEC 7813	*Identification cards - Financial transaction cards*
ISO/IEC 10373	*Identification cards - Test methods*
ISO/IEC 24727	*Identification cards - Integrated circuit card programming interfaces*
ISO/IEC 19784	*Information technology - Biometric application programming interface*
ISO/IEC 14443	*Identification cards - Contactless integrated circuit cards - Proximity cards*
ISO/IEC TR 29123	*Proximity Cards - Requirements for the enhancement of interoperability*
ISO 19785	*Information technology - Common Biometric Exchange Formats Framework*
ISO 19794	*Information technology - Biometric data interchange formats*
ISO 29109	*Information technology - Conformance testing methodology for biometric data interchange formats*
ISO 24745	*Information technology - Security techniques - Biometric information protection*
ISO 30136	*Biometric information protection (em desenvolvimento)*
ISO/IEC 8824	*Information technology - Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825	*Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules*
ISO 8372	*Information processing - Modes of operation for a 64-bit block cipher algorithm*
ISO/IEC 15946	*Information technology - Security techniques - Cryptographic techniques based on elliptic curves*
ISO/IEC 9797	*Information technology - Security techniques - Message Authentication Codes (MACs)*
ISO/IEC 9796	*Information technology - Security techniques - Digital signature schemes giving message recovery*
ISO/IEC 14888	*Information technology - Security techniques - Digital signatures with appendix*
ISO/IEC 10118	*Information technology - Security techniques - Hash-functions*
ISO 9992	*Financial transaction cards - Messages between the integrated circuit card and the card accepting device*
ISO/IEC 9798	*Information technology - Security techniques - Entity authentication*
ISO/IEC 3309	*Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Frame structure*
ISO/IEC 9594-8	*Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*
ISO 10202-1	*Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 1: Card life cycle*
ISO 8583	*Financial transaction card originated messages - Interchange message specifications*
ISO/IEC 15408	*Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria)*
ISO/IEC 15438	*Information technology -- Automatic identification and*

	data capture techniques -- PDF417 bar code symbology specification
ISO/IEC 18004	*Information technology -- Automatic identification and data capture techniques -- QR Code 2005 bar code symbology specification*
ISO/IEC 24713-1	*Information technology -- Biometric profiles for interoperability and data interchange - Part 1: Overview of biometric systems and biometric profiles*
ISO/IEC 24713-2	*Information technology -- Biometric profiles for interoperability and data interchange -- Part 2: Physical access control for employees at airports*
ISO/IEC 24713-3	*Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers*

b. Comitê Europeu de Normatização (CEN):

Norma	Descrição
CEN TS 15480	*Identification card systems European Citizen Card*
CEN CWA 14890	*Application Interface for smart cards used as Secure Signature Creation Devices*
CEN EN 1546-3	*Identification Card Systems - Inter-Sector Electronic Purse*
ENV 1292	*Identification card systems. Integrated circuit(s) cards and interface services. Additional test methods*
EN 1545	*Identification card systems. Surface transport applications*
EN 15320	*Identification card systems - Surface transport applications - Interoperable public transport applications – Framework*
ENV 14062	*Identification card systems - Surface transport applications - Electronic fee collection*
EN 28583	*Financial Transaction Card Originated Messages - Inter-*

	change Message Specifications
DS CEN/CR 1750	*Identification Card Systems - Inter-Sector Messages Between Devices And Hosts - Acceptor To Acquirer Messages*

c. ETSI (*European Telecommunications Standards Institute*):

Norma	Descrição
TS 42.009	*Digital cellular telecommunications system (Phase 2+) Security aspects*
TS 42.017	*Digital cellular telecommunication system (Phase 2+) Subscriber Identity Modules (SIM) Functional characteristics*
TS 42.019	*Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API)*
TS 42.048	*Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM application toolkit*
TS 43.019	*Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API) for Java Card*
TS 43.048	*Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit*
TS 51.011	*Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface*
TS 51.013	*Digital cellular telecommunications system Test specification for Subscriber Identity Module (SIM) Application Programming Interface (API) for Java Card*
TS 51.014	*Digital cellular telecommunications system Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM–ME) interface*
TS 51.017	*Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module (SIM) test specification*
TS 35206	*Specification of the MILENAGE Algorithm Set: An example alghorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3,f4,f5 and f5**
TS 43048	*Biblioteca criptográfica*
TS 102221	*Smart Cards UICC-Terminal interface Physical and logical characteristics*
TS 102600	*Smart Cards; UICC- Terminal interface; Characteristics of the USB interface*
TS 102613	*Smart Cards; UICC - Contactless Front- end (CLF) Interface*
TS 102622	*Smart Cards; UICC - Contactless Front-end (CLF) interface; Host Controller Interface (HCI)*
TS 102222	*Integrated Circuit Cards (ICC);Administrative commands for telecommunications applications*

d. ITU-T (*Telecommunication Standardization Sector of ITU*):

Norma	Descrição
X.409	*Abstract Syntax Notation Definition*
X.500	*Data Networks, opens systems communications and security*
X.509	*Data Networks, opens systems communications and security The Directory Public-Key and attribute certificate frameworks*
X.690	*Data Networks, opens systems communications OSI networking and systems aspects- Abstract Syntax Notation One (ASN.1)*

e. ANSI (*American National Standard Institute*):

Norma	Descrição
X9.17	*Financial Institution Key Management*
X9.30-2	*Public Key Cryptography Using Irreversible Algorithms - Part 2: The Secure Hash Algorithm (SHA-1)*
X9.31	*RSA signature schemes*

f.EMV (*Europay, MasterCard and Visa*)

Norma	Descrição
EMV 4.3 Book 1	*Application Independent ICC to Terminal Interface Requirements*
EMV 4.3 Book 2	*Security and Key Management*
EMV 4.3 Book 3	*Application Specification*
EMV 4.3 Book 4	*Cardholder, Attendant, and Acquirer Interface Requirements*

g. Internet Engineering Task Force

Norma	Descrição
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*

RFC 1750	*Randomness Recommendations for Security*
RFC 2246	*The TLS Protocol*
RFC 2818	*HTTP Over TLS*
RFC 3163	*ISO/IEC 9798-3 Authentication SASL Mechanism*
RFC 3447	*Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography*
RFC 2898	*PKCS #5: Password-Based Cryptography Specification Version 2.0*
RFC 2315	*PKCS #7: Cryptographic Message Syntax*
RFC 5208	*Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification*
RFC 2985	*PKCS #9: Selected Object Classes and Attribute Types*
RFC 2986	*PKCS #10: Certification Request Syntax Specification*
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
RFC 3370	*Cryptographic Message Syntax (CMS) Algorithms*
RFC 3369	*Cryptographic Message Syntax (CMS)*
RFC 2527	*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*
RFC 1510	*The Kerberos Network Authentication Service (V5)*
RFC 3023	*XML Media Types*

h. ICAO

Norma	Descrição
Doc 9303 Part 3 Vol 1	*MRtds with Machine Readable Data* *Stored in Optical Character Recognition Format*
Doc 9303 Part 3 Vol 2	*Specifications for Electronically Enabled MRtds* *with Biometric Identification Capability*
Technical Report	*Machine Readable Travel Documents GUIDANCE DOCUMENT PKI for Machine Readable Travel Documents*
Technical Re-	*Supplement to ICAO Doc 9303 - Release10*

port	
Technical Report	*Supplement to ICAO Doc 9303 - Release11*
Technical Report	*Supplement to ICAO Doc 9303 - Release12*
Technical Report	*Supplement to ICAO Doc 9303 - Release14*
Technical Report	*Supplemental Access Control for Machine Readable Travel Documents*
Technical Report	*Durability of Machine Readable Passports*
Technical Report	*PKI for Machine Readable Travel Documents offering ICC Read-Only Access*

i. RSA DataSecurity Inc. (EMC Corporation):

Norma	Descrição
PKCS #1	*RSA Standard: Defines RSA public and private keys (ASN.1-encoded in clear-text), basic algorithms and encoding/padding schemes, and producing and verifying signatures. (RFC 3447)*
PKCS #3	*Diffie–Hellman Key Agreement Standard:*
PKCS #5	*Password-based Encryption Standard.(RFC 2898, PBKDF2).*
PKCS #6	*Extended-Certificate Syntax Standard: Defines extensions to the obsolete v1 X.509 certificate specification.*
PKCS #7	*Cryptographic Message Syntax Standard: Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination. Formed the basis for S/MIME(RFC 5652), an updated Cryptographic Message Syntax Standard(CMS). Often used for single sign-on. (RFC 2315)*
PKCS #8	*Private-Key Information Syntax Standard: Used to carry private certificate keypairs (encrypted or unencrypted).*

	(RFC 5208)
PKCS #9	*Selected Attribute Types. Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests. (RFC 2985)*
PKCS #10	*Certification Request Standard: Format of messages sent to a certification authority to request certification of a public key. (RFC 2986)*
PKCS #11	*Cryptographic Token Interface: Also known as "Cryptoki". An API defining a generic interface to cryptographic tokens (Hardware Security Module). Used in single sign-on, public-key cryptography and disk encryption systems. RSA Security has turned over further development of the PKCS#11 standard to the OASIS PKCS 11 Technical Committee.*
PKCS #12	*Personal Information Exchange Syntax Standard: Defines a format to store private keys with public key certificates, protected with a symmetric key. PFX is a predecessor to PKCS #12. This container can contain multiple certificates, encrypted with a password. Usable as a format for the Java key store and for client authentication in Mozilla Firefox, and by Apache Tomcat.*
PKCS #15	*Cryptographic Token Information Format Standard: Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15.*

j. IEEE:

Norma	Descrição
1363	*Standard Specifications for Public Key Cryptography*
1363 Amndt 1	*Standard Specifications for Public Key Cryptography: Additional Techniques*

k. Calypso (*International electronic ticketing standard for contactless smart cards, originally designed by a group of European transit operators*):

Norma	Descrição

100324	*CALYPSO Handbook*
010608	*CALYPSO FUNCTIONAL SPECIFICATION Card Application*
FP01	*SAM and Key Management*

l. BSI (*Bundesamt für Sicherheit in der Informationstechnik/*Escritório Nacional para Segurança da Informação):

Norma	Descrição
TR-03127	*Architecture electronic Identity Card and electronic Resident Permit*
BSI-CC-PP-0064	*Common Criteria Protection Profile for Inspection Systems (IS)*
TR-03110	*Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*
TR-03110-1	*Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1*
TR-03110-2	*Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*
TR-03110-3	*Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications*
TR-03112-1	*eCard-API-Framework – Overview*
TR-03112-2	*eCard-API-Framework – eCard-Interface*
TR-03112-3	*eCard-API-Framework – Management-Interface*
TR-03112-4	*eCard-API-Framework – ISO 24727-3-Interface*
TR-03112-5	*eCard-API-Framework – Support-Interface*
TR-03112-	*eCard-API-Framework – IFD-Interface*

6	
TR-03112-7	*eCard-API-Framework – Protocols*
TR-03121-1	*Biometrics for Public Sector Applications Part 1: Framework*
TR-03121-2	*Biometrics for Public Sector Applications Part 2: Software Architecture and Application Profiles*
TR-03121-3	*Biometrics for Public Sector Applications Part 3: Function Modules*
TR-03130-1	*Technical Guideline eID-Server Part 1: Functional Specification*
BSI TR-03130-2	*Technical Guideline eID-Server Part 2: Security Framework*
AIS20/AIS 31	*A proposal for: Functionality classes for random number generators*
BSI-CC-PP-0066-V2	*Common Criteria Protection Profile eID-Client based on eCard-API*
--	*Security Aspects and Prospective Applications of RFID Systems*

m. *International Labour Organization* (ILO):

Norma	Descrição
LO SID-0002	*Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)*

n. US DHS *(Department of Homeland Security)*

Norma	Descrição
---	*TWIC Reader Hardware and Card Application Specification May 2012*

o. OASIS

Norma	Descrição

--	*Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*
--	*Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*

p. PC/SC: *Interoperability Specification for ICCs and Personal Computer Systems*

Norma	Descrição
--	*Part 1. Introduction and Architecture Overview*
--	*Part 2. Interface Requirements for Compatible IC Cards and Readers*
--	*Part 3. Requirements for PC-Connected Interface Devices*
--	*Part 3. Requirements for PC-Connected Interface Devices Amndt 1*
--	*Part 3. Supplemental Document*
--	*Part 3. Supplemental Document for Contactless ICCs*
--	*Part 4. IFD Design Considerations and Reference Design Information*
--	*Part 5. ICC Resource Manager Definition*
--	*Part 6. ICC Service Provider Interface Definition*
--	*Part 7. Application Domain and Developer Design Considerations*
--	*Part 8. Recommendations for ICC Security and Privacy Devices*
--	*Part 9. IFDs with Extended Capabilities*
--	*Part 10 IFDs with Secure PIN Entry Capabilities*
--	*Part 10 IFDs with Secure PIN Entry Capabilities Supplement - IFDs with Feature Capabilities*

--	*Part 10 IFDs with Secure PIN Entry Capabilities AMNT 1*

q. NIST

Norma	Descrição
NISTR 7870	*NIST Test Personal Identity Verification (PIV) Cards*
--	*Technical Specifications for Personal Identity Verification (PIV) Test Cards*
FIPS PUB 201-2	*Personal Identity Verification (PIV) of Federal Employees and Contractors*
SP 800-168	*Approximate Matching: Definition and Terminology*
SP 800-161	*Guide to Attribute Based Access Control (ABAC) Definition and Considerations*
NISTIR 8014	*Considerations for Identity 5 Management in Public Safety 6 Mobile Networks (DRAFT)*
SP 800-79-2	*Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*
FIPS PUB 202	*SHA Standard: Permutation Based Hash and Extendable Output Functions*
SP 800-78-4	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
SP 800-73-3	*Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application*
SP 800-73-3	*Interfaces for Personal Identity Verification – Part 2: End-Point PIV Card Application Card Command Interface*
SP 800-73-3	*Interfaces for Personal Identity Verification – Part 3: End-Point PIV Client Application Programming Interface*
SP 800-73-3	*Interfaces for Personal Identity Verification – Part 4: The PIV Transitional Interfaces and Data Model Specification*
SP 800-73-4 Part 1	*Interfaces for Personal Identity Verification Part 1: PIV Card Application Namespace, Data Model and Representation*
SP 800-73-4 Part 2	*Interfaces for Personal Identity Verification Part 2: PIV Card Application Card Command Interface*
SP 800-76-2	*Biometric Specifications for Personal Identity Verification*
SP 800-73-4 Part 3	*Interfaces for Personal Identity Verification Part 3: PIV Client Application Programming Interface*

SP 800-104	*A Scheme for PIV Visual Card Topography*
SP 800-116	*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
SP 800-85A-2	*PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 compliance)*
SP 800-85B	*PIV Data Model Test Guidelines*
SP 800-85B-1	*PIV Data Model Test Guidelines*
SP 800-96	*PIV Card to Reader Interoperability Guidelines*
SP 800-63-2	*Electronic Authentication Guideline*
SP 800-63-1	*Electronic Authentication Guideline*
SP 800-57 Part 3	*Recommendation for Key Management*
SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
SP 800-16	*A Role -Based Model for Federal Information Technology/ Cybersecurity Training*
SP 800-98	*Guidelines for Securing Radio Frequency Identification (RFID) Systems*
SP 80-56B	*Recommendation for Pair –Wise Key Establishment Schemes Using Integer Factorization Cryptography*
SP 800-157	*Guidelines for Derived Personal Identity Verification (PIV) Credentials*
NISTIR 7981	*Mobile, PIV and Authentication*
NISTR 7977	*NIST Cryptographic Standards and Guidelines Development Process*
SP 800-152	*A Profile for U. S. Federal Cryptographic Key Management Systems*
NISTIR 7863	*Cardholder Authentication for the PIV Digital Signature Key*
NISTIR 6867	*Government Smart Card Interoperability Specification*
SP 800-38G	*Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*
SP 800-90C	*Recommendation for Random Bit Generator (RBG) Constructions*
SP 800-85B-1	*PIV Data Model Test Guideline*
SP 800-103	*An Ontology of Identity Credentials Part 1:Background and Formulation*
SP 800-133	*Recommendation for Cryptographic Key Generation*
SP 800-	*Transitions: Recommendation for Transitioning the Use*

131A	*of Cryptographic Algorithms and Key Lengths*
SP 800-116	*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
SP 800-108	*Recommendation for Key Derivation Using Pseudorandom Functions*
NISTIR 8014	*Considerations for Identity Management in Public Safety Mobile Networks (DRAFT)*
NISTIR 7849	*A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification*
SP 800-107	*Recommendation for Applications Using Approved Hash Algorithms*
SP 800-106	*Randomized Hashing for Digital Signatures*
FIPS 186-4	*Digital Signature Standard (DSS)*
FIPS 180-4	*Secure Hash Standard (SHS)*
FIPS 140-2	*SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*
FIPS 140-2 Annex C	*Approved Random Number Generators for FIPS PUB 140 -2*
FIPS 140-2 Annex D	*Approved Key Establishment Techniques for FIPS PUB 140-2*
FIPS 197	*Advanced Encryption Standard*

r. Common Criteria

Norma	Descrição
2006-06-001	*Rationale for Smart cards and similar devices*
CCDB-2010-03-001	*Guidance for smartcard evaluation v2.0*
CCDB-2014-04-001	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices*
CCDB-2009-03-002	*Application of CC to Integrated Circuits v3.0*
CCDB-2012-04-001	*Composite product evaluation for Smartcards and similar devices v1.2*
CCDB-2007-09-02	*ETR-template lite for composition v1.0*
CCDB-2012-04-003	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices*
CCDB-2012-04-004	*Security Architecture requirements (ADV_ARC) for smart cards and similar devices - Appendix 1*
CCDB-2013-05-001	*Requirements to perform Integrated Circuit Evaluations*
CCDB-2013-05-002	*Application of Attack Potential to Smartcards*

CCMB–2012-09-001	*Part 1: Introduction and general model*
CCMB–2012-09-002	*Part 2: Security functional components*
CCMB–2012-09-003	*Part 3: Security assurance components*
CCMB-2012-09-004	*Evaluation methodology*

s. *GlobalPlataform*

Norma	Descrição
GPC_SPE_031	*Composition Model*
GPC_GUI_050	*Composition Model Security Guidelines for Basic Applications*
GPC_SPE_055	*Card Specification – ISO Framework*
GP_REQ_004	*Requirements for NFC Mobile: Management of Multiple Contactless Secure Elements*
GPC_SPE_007	*Confidential Card Content Management Card Specification v2.2 - Amendment A*
GPC_SPE_032	*Card Specification v2.2.1 GlobalPlatform on MULTOS™ API*
GPC_SPE_025	*Contactless Services Card Specification v2.2 – Amendment C*
GPC_SPE_014	*Secure Channel Protocol 03 card Specification v 2.2 – Amendment D*
GPC_SPE_042	*Card Specification v 2.2 – Amendment E*

t. FUTURE ID

Norma	Descrição
WP32- eID Services	*Interface and Module Specification for eID Services*
WP32- eID Services	*Implementation of Basic and Generic Modules*
WP42 - Universal Authentication Service	*Interface and Module Specification and Documentation*

2.2 Grupos e institutos de pesquisa sobre temas relativos a eID´s

Com o mesmo objetivo de auxiliar o trabalho de especificação do RIC e a busca de cooperação técnica, foi realizada uma investigação acerca de grupos de pesquisa sobre identidade eletrônica, gerenciamento de identidade, privacidade em identidades, protocolos de autenticação, interoperabilidade de esquemas de identidade, interoperabilidade de *smartcards* e segurança física dos *smartcards*. A maior parte dos grupos de pesquisas encontra-se na Europa, onde vários países já lançaram esquemas de eID, e buscam a interoperabilidade entre os modelos.

a. Segurança física dos *chips*:

Grupo	Descrição
Fraunhofer SIT (Alemanha)	O *Fraunhofer Institute for Secure Information Technology* possui laboratório (*Applied and Integrated Security AISEC*) para ensaio de ataques físicos a *chips* e propõe também esquemas de proteção física. Pesquisadores: Michael Kasper, Frederic Stumpf. https://www.sit.fraunhofer.de/
CASED (Alemanha)	O CASED (*Center for Advanced Security Darmstadt*) desenvolve pesquisas nas áreas de segurança física, criptografia e privacidade. http://www.cased.de/en/research.html
Infineon Technologies	Possui grupo de pesquisa sobre o assunto: *Chip Card, Security Innovation Group* http://www.infineon.com/cms/en/product/

b. Protocolos de autenticação, recursos de privacidade, modelos de gerenciamento de identidade, interoperabilidade de eID:

Grupo	Descrição
ENISA (Grécia)	A ENISA (*European Union Agency for Network and Information Security*) é um órgão de capacitação referente a segurança da informação da União Europeia e desenvolve trabalhos sobre privacidade e segurança de eID´s http://www.enisa.europa.eu/
IPTS (Espanha)	O IPTS (*Institute for Prospective Technological Studies*) faz parte da rede de institutos de pesquisa (JRC) da Comissão Europeia (EC) e desenvolveu estudos sobre o uso de eID na Europa. https://ec.europa.eu/jrc/en/institutes/ipts
Porvoo	O Grupo de Porvoo é uma rede internacional de

Group (Finlândia)	cooperação, cujo objetivo principal é promover uma identidade eletrônica transnacional e interoperável baseada em tecnologia PKI (*Public Key Infrastructure*) e *smartcards* e cartões de chip de identificação, a fim de ajudar a garantir, a setores público e privado, a segurança de operações na Europa. http://www.fineid.fi/default.aspx?id=539
OECD ICCP/WPISP (França)	Desenvolve estudos sobre privacidade, segurança, identificação por rádio frequência (RFID), gerência de identidade digital, http://www.oecd.org/sti/ieconomy/informationsecurityandprivacy.htm
ITIF (EUA)	A *Information Technology and Innovation Foundation* (ITIF) é um instituto de pesquisa para promoção de políticas públicas ligadas a inovação e tecnologia, e desenvolveu estudos sobre o uso de eID no mundo e fez recomendações para o EUA. http://www.itif.org/
Fraunhofer IAO (Alemanha)	Participa do projeto *Future ID*. http://www.iao.fraunhofer.de/lang-en/component/content/article/99-information-communication-technology/iao-news/1020-future-id.html

c. Interoperabilidade de *smartcard*

PC/SC Workgroup (Aberto)	Elabora especificações para garantir interoperabilidade de *smartcards* e leitoras de diferentes fabricantes. http://www.pcscworkgroup.com/index.php?h
Global Plataform (EUA)	Desenvolve especificações para promover uma interoperabilidade segura de tecnologias de chip. Possui um comitê específico par *smartcard*, liderado pela G&D. http://www.globalplatform.org/aboutusmission.asp

No Brasil a pesquisa sobre temas relacionados a eID é quase inexistente. Pode-se citar o grupo de pesquisa e desenvolvimento de gerenciamento de identidades federadas, liderado pela Prof. Michele S. Wangham da UNIVALE.

Com relação à produção acadêmica nacional sobre eID pode-se citar:

- dissertação de mestrado de 2007, de YAMAR AIRES DA SILVA do Departamento de Engenharia Elétrica da Universidade de Brasília, sob a orientação do professor RICARDO STACIARINI PUTTINI, intitulada: ESTUDO

E PROPOSTA DE UM NOVO DOCUMENTO DE IDENTIFICAÇÃO ELETRÔNICA (e-ID) PARA O BRASIL, que faz uma revisão sobre as normas referentes a *smartcards*, ataques e proteção contra ataques físicos, processos de fabricação, certificação digital e faz uma proposta de documento eletrônico.

Considerando a possibilidade de cooperação internacional, pode-se citar o Instituto de Pesquisas Tecnológicas, que apesar de não possuir projetos relacionados a eID, já desenvolveu outros projetos em cooperação com o Instituto Fraunhofer, que, conforme supracitado, possui grupo de trabalho e participa de diversos projetos sobre eID.

Na área de desenvolvimento e testes em *smartcards,* pode-se citar:

- LEA (Laboratório de Ensaios e Auditoria) do LSI-TEC (Laboratório de Sistemas Integráveis Tecnológico) em São Paulo-SP: credenciado pelo ITI para homologação de cartões e equipamentos da ICP-Brasil.

- Laboratório de Estudos e Aplicações de RFID do CPqD (Centro de Pesquisa e Desenvolvimento) em Campinas-SP: possui laboratório e realiza testes descritos pela norma ISO 10373.

Com relação à produção acadêmica nacional sobre *smartcards*, protocolos de autenticação e *middlewares*, pode-se citar:

- dissertação de mestrado de 2009 de JOSÉ MARIA LEOCÁDIO do Departamento de Engenharia Elétrica da Universidade de Brasília, sob a orientação do professor ANDERSON CLAYTON ALVES NASCIMENTO, intitulada: APLICAÇÃO DE SEGURANÇA ELETRÔNICA COM JAVA CARDS: O CASO DE UM PROTOCOLO PARA REGISTRO ON LINE E SEM ANONIMATO EM CARTÕES CRITOGRAFICAMENTE INTELIGENTES, que faz uma revisão sobre as biblioteca criptográfica pertinente, tecnologia *smartcard*, sistemas operacionais, ataques e proteção contra ataques físicos, processos de fabricação, protocolos de autenticação para pagamento, e propõe uma adaptação ao protocolo cSET.

- tese de doutorado de 2012 de BRUNO EMERSON GURGEL GOMES da Pós Graduação em Ciências da Computação da UFRN, sob a orientação do professor DAVID BORIS PAUL DEHARBE, intitulada: DESENVOLVIMENTO FORMAL DE APLICAÇÕES PARA SMART CARD, que faz uma revisão sobre tecnologia *smartcard*, *Javacard*, modelos de especificação e tradução para *Javacard* e um estudo de caso sobre aplicação no passaporte.

- tese de doutorado de 2009 de JOSÉ ANTÔNIO CARRIJO BASRBOSA do Departamento de Engenharia Elétrica da Universidade de Brasília, sob a orientação do professor ANDERSON CLAYTON ALVES NASCIMENTO, intitulada: CRIPTOANÁLISE DE PROTOCOLOS DIRECIONADOS A DISPOSITIVOS DE BAIXO PODER COMPUTACIONAL, que faz uma revisão sobre a biblioteca criptográfica pertinente, tecnologia *smartcard*, protocolos HB e propõe novos ataques a estes protocolos.

2.3 Projetos referentes a eID´s

Vários projetos de pesquisa sobre eID, abordando assuntos como interoperabilidade, privacidade e segurança são litados em [4]. Uma lista mais atual e completa é mostrada abaixo:

Projeto	Descrição
IDABC eID *Interoperability for* PEGS	Desenvolvido pela IDABC (*Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens*) da Comissão Europeia, o projeto, concluído em 2009, aborda o problema de interoperabilidade entre os modelos de eID, com pesquisa sobre eID e com levantamento de padrões dos diversos países da Europa, propostas de soluções e especificações comuns para interoperabilidade. http://ec.europa.eu/idabc/en/document/6484.html
FUTURE ID	O projeto, coordenado pelo Instituto Fraunhofer, englobando países como Áustria, Bélgica, Dinamarca, Estônia, França, Alemanha, Noruega, Polônia, Espanha, Suíça e Reino Unido, tendo como parceiros IBM, Infineon e G&D entre outros, iniciou-se em 2012 e tem término previsto para 2015. Propõe desenvolver uma infraestrutura de gerenciamento de identidade para toda Europa, com recursos de privacidade,

	integrando a infraestrutura já existente e os serviços emergentes de modelos de identidade federada, provendo um sistema centrado no usuário. http://www.futureid.eu/
STORK (*Secure idenTity acrOss boRders linKed*) 2	Continuação projeto STORK, expandido para 19 países da União Europeia, contando com 58 parceiros institucionais como ministérios e universidades, propõe uma integração dos processos de identificação eletrônica e autenticação na Europa, elaborando especificações e padronizações de processos e componentes de sistemas, e coordenando pilotos. https://www.eid-stork2.eu/
CROBIES (*Cross-Border Interoperability of eSignatures*)	Iniciado em 2008 e finalizado em 2010, coordenado pela Comissão Europeia, visava propor soluções para interoperabilidade de assinaturas eletrônicas qualificadas e avançadas no âmbito da Europa. http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm
PRIME (*Privacy and Identity Management for Europe*)	Iniciado em 2004 e finalizado em 2008, envolvendo 20 membros como universidades, IBM e HP, visou a desenvolver o protótipo de trabalho para sistemas de gerenciamento de identidade com mecanismos de privacidade. https://www.prime-project.eu/
PrimeLife	Iniciado em 2008 e finalizado em 2011, fundado dentro da Comissão Européia, contando com parceiros como universidades, IBM e Microsoft, abordou assuntos de privacidade e gerenciamento de identidade, dando continuidade ao projeto PRIME. http://www.primelife.eu/
PICOS (*Privacy and Identity Management for Community Services*)	Iniciado em 2008 e finalizado em 2011, contando com 11 parceiros como universidades e IBM, visava a construção de uma plataforma para provisão de privacidade e confiança e gerenciamento de identidades para serviços e aplicações na Internet e redes móveis de comunicações. http://www.picos-project.eu/
Privacy OS	Iniciado em 2008 e finalizado em 2010, coordenado pelo Centro Independente de Proteção à Privacidade (Alemanha), envolvendo uma rede de universidades e agência

	governamentais sob a Comissão Europeia, visava fomentar o desenvolvimento de infraestruturas de privacidade na Europa. https://www.privacyos.eu/
Modinis IDM	Iniciado em 2005 e finalizado em 2007, com participação do A-SIT (Áustria) e a Universidade de Leuven (Bélgica), visava desenvolver conhecimento sobre gerenciamento de identidades no governo eletrônico na Europa. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
TURBINE (*Trusted Revocable Biometric IdeNtitiEs*)	Iniciado em 2008 e já finalizado, visava desenvolver técnicas de proteção à privacidade da biometria, com o emprego de pseudo-identidades revogáveis e não vulneráveis a engenharia reversa, com desempenho compatível com os algoritmos atuais. http://www.turbine-project.eu/
BEST (*Biometrics European Stakeholders Network*)	Iniciado em 2011, a rede coordenada pelo Instituto Fraunhofer, contando com 26 parceiros como universidades, dividida em 7 grupos de trabalho com biometria em eID, visa captar conhecimento sobre uso de biometria na Europa, propor e disseminar recomendações de boas práticas. http://www.best-nw.eu/
ABC4Trust (*Attribute-based Credentials for Trust*)	Iniciado em 2012, contando com 16 membros como a IBM e a Microsoft, visa realizar pesquisa e desenvolvimento de tecnologias suportando Credenciais baseadas em Atributos com preservação de privacidade (Privacy-ABC). https://abc4trust.eu/
SEMIRAMIS (*Secure Management of Information across multiple Stakeholders*)	Iniciado em 2010 e finalizado em 2012, envolvendo 9 membros como universidades europeias, visou definir uma infraestrutura piloto para serviços eletrônicos com requisitos de autenticação segura e realizar testes sob diversos cenários. http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=250453
FIDIS (*Future of Identity in the*	Iniciado em 2005 e finalizado em 2009, composto pela IBM, agências como a JRC, e universidades da Europa, visava reformular os requisitos para um gerenciamento de identidade futuro na Europa e contribuir com as tecnologias e

Information Society)	infraestruturas necessárias. http://www.fidis.net/
SSEDIC	Rede, coordenada pela Universidade Vergata de Roma, com mais de 30 parceiros como A-SIT e Instituto Fraunhofer e mais de 200 experts sobre eID, visa estabelecer recomendações relativas a usabilidade e a interoperabilidade de soluções de gerenciamento de identidade eletrônica na Europa, com quatro grandes áreas: eID móvel, uso de atributos, autenticação e suscetibilidade. http://www.eid-ssedic.eu/
PETWEB II (*Privacy-respecting Identity Management for e-Norge*)	Iniciado em 2009 e finalizado em 2013, coordenado pela Universidade de Gjøvik em parcerias com agências e universidades da Noruega, Suécia e Holanda, abordou aspectos sociais relativos a identificação eletrônica, como percepção de privacidade e efeitos criminais. http://petweb2.projects.nislab.no/index.php/Main_Page
Skydentity	Iniciado em 2011, contando com 9 parceiros como o Instituto Fraunhofer, visa construir uma ponte entre eID´s e as infraestruturas emergentes e existentes de computação nas nuvens. https://www.skidentity.com/en/objective/
GINI-SA(*Global Identity Networking of Individuals - Support Action*)	Iniciado em 2009, contando com 8 parceiros de países europeus, com universidades e o Instituto Fraunhofer, visa investigar e estabelecer bases para uma arquitetura e de aspectos de privacidade de serviços relacionados ao gerenciamento de identidade centrado no usuário. O projeto trabalha na direção de uma visão de um ambiente de gerenciamento de identidade individual onde os indivíduos serão capazes de gerenciar seu próprio espaço de identidade. http://www.gini-sa.eu/index.php?option=com_content&view=frontpage&Itemid=1
Open eID	Coordenado pelo Instituto Fraunhofer dentro do SourceForge, o projeto fornece uma implementação Java dos protocolos PACE, autenticação de Terminal e autenticação de Chip, que são usados pela infra-estrutura das novas carteiras de identidade alemães. Este projeto, além disso, fornece uma implementação cliente Android eID.

	http://sourceforge.net/projects/open-eid/

2.4 Projetos de interoperabilidade de *smartcards*

Projeto	Descrição
OpenSCDP(*Open Smart Card Development Platform*)	O Opencard Framework é um *middleware* de *smartcard* em Java, para APDUs com e sem contato, conforme definido pela norma ISO/IEC 7816-4/8/9. O consórcio OpenCard, com IBM e Gemplus concluiu a versão 1.2 da especificação e uma implementação e foi encerrado em 2007. O código original foi transferido a um projeto no SourceForge, mas não foi mantido ativamente. O OPenSCDP é uma coleção de ferramentas para o desenvolvimento, teste e implantação de aplicativos de infra-estrutura de chaves públicas do smart card. Ele usa as capacidades de Plataforma Global. http://www.openscdp.org/ocf/index.html
OpenSC	OpenSC é um código aberto escrito por uma equipe internacional de voluntários, além da ZETES. Fornece bibliotecas e utilitários para *smartcards* que suportam as operações de criptografia, para facilitar o seu uso em aplicações de segurança, como autenticação, criptografia de e-mail e assinaturas digitais. Implementa a API PKCS # 11 (compatível com Mozilla Firefox). No cartão o OpenSC implementa o padrão PKCS # 15. Seu código é utilizado como base para aplicativos de eID como o aplicativo oficial do Belpic (eID Belga). https://github.com/OpenSC/OpenSC/wiki
Open eCard	Um código aberto escrito por uma equipe internacional de voluntários além de membros do FutureID. O objetivo do eCard-API-Framework é o fornecer uma interface simples e homogênea de código aberto da API baseada nas especificações BSI-TR3112, para permitir o uso padronizado dos vários *smartcard* para diferentes aplicações *smartcards* para autenticação e para assinatura. https://www.openecard.org/en/ecard-api-framework/overview/

2.5 Infraestrutura tecnológica para a produção de eID´s

Este tópico visa também fornecer uma visão geral, por meio de uma pesquisa não exaustiva, da infraestrutura existente para a produção de eID´s, *smartcards*, *chips* e desenvolvimento de *softwares* como *middlewares* e algoritmos de *Match on Card* (MOC).

a. No mundo:

1) Fabricantes de *chips* padrão ISO/IEC 7816 e ISO/IEC 14443

- Infineon Technologies: Atual líder de mercado na produção de *chips* para a aplicação de eID, com participação em mais da metade dos projetos de eID, desenvolve tecnologias, como a *Integrity Guard* (com criptografia dos registros da CPU), e produz *chips* nos padrões ISO/IEC 7816 e ISO/IEC 14443 aplicadas a ePassaporte, eID, e cartões eletrônicos de saúde (eSaúde). Também possui centros de pesquisa de tecnologias em segurança contra ataques físicos ao *chip*.

http://www.infineon.com/cms/en/product/applications/chip-card-and-security/govid.html

- NXP Semiconductors: produz *chips* para a aplicação de eID, desenvolve tecnologias, como a *SmartMX e SmartMX2*, e produz *chips* nos padrões ISO/IEC 7816 e ISO/IEC 14443 aplicadas a ePassaporte, eID, e cartões eSaúde.

http://www.nxp.com/applications/egovernment/national-id.html

- SAMSUNG: produz *chips* nos padrões ISO/IEC 7816 da linha FSID (Financial Security and Identification).

http://www.samsung.com/global/business/semiconductor/product/security-solution/overview

- ST Microelectroncs: produz *chips* nos padrões ISO/IEC 7816 para aplicação de eID, e-passaporte e cartão eSaúde, com a plataforma ST23.

http://www.st.com/st-web-

ui/static/active/en/resource/sales_and_marketing/promotional_material/flyer/FLEGOVER1111.pdf?s_searchtype=keyword

2) Fabricantes de cartões ID-1 com *chip* e integração de tecnologia:

- GEMALTO: atua na produção de e-passaportes, eID, cartões eSaúde, com pacotes de solução integrada como Sealys para a produção de documentos e a solução Coesys para sistemas de cadastro, emissão, gerenciamento e verificação de identidade.

  http://www.gemalto.com/govt/customer_cases/index.html#eid

- Giesecke & Devrient: atua na produção de e-passaportes, eID, cartões eSaúde, com pacotes de solução integrada. Oferecem diversas implementações para sistemas operacionais sob normas e certificações internacionais de segurança. A G&D oferece dois tipos de sistema operacional, que constituíram os sistemas de ponta com respeito à segurança nas últimas décadas e atendem todas as normas internacionais: STARCOS, como sistema operacional nativo (satisfaz a norma ISO/IEC 7816), e o Sm@rtCafé Expert, como sistema operacional padronizado JavaCard.

  https://www.gi-de.com/pt/products_and_solutions/products/national_id_cards/Documentos-de-identidade-nacionais-para-identifica%C3%A7%C3%A3o-segura-6530.jsp

- Oberthur Technologies: atua na produção de eID´s e e-passaportes.

  http://www.oberthur.com/otsolutions/digital-identity/?lang=en

- Muhlbauer: produz equipamentos de fabricação de cartões ID-1 e atua na produção de eID´s com pacotes de solução integrada como TIDIS (*Mühlbauer's Tecurity Identity Document Issuance*) para cadastramento e gerenciamento, produção, personalização e verificação de identidade.

- Safran Morpho: atua na produção de epassaportes, eID, cartões e-Saúde, com pacotes de solução integrada para cadastramento, produção e personalização, emissão, gerenciamento e verificação de identidade. Possui uma solução para eID na plataforma Ideal Citiz.
  http://www.morpho.com/e-documents/id-documents/products/id-cards-and-resident-cards/?lang=en

- Valid: possui diversas subsidiárias e atua na produção cartões EMV, certificação digital e meio de pagamento.

  http://www.valid.com.br/a-companhia/empresas-grupo

- Bundesdruckerei (BUDRU): empresa pública alemã que atua na produção de e-passaportes, carteiras de motorista e eID da Alemanha. Também oferece soluções para cadastramento, personalização, emissão e verificação de identidade.
  https://www.bundesdruckerei.de/en/1544-solutions-products

- Trüb AG: Produz cartões de identidade sem *chip* ou *smartcards* multifuncionais com base na solução de Java da Trub para o e-governo, com tecnologias com contato, sem contato, dual-interface ou mesmo híbrido, em policarbonato. O portfólio de aplicativos inclui infraestrutura de chave pública (PKI) *applet* e *middleware*, a função eMRTD com as normas da ICAO, e aplicações sob medida para cada cliente. Além de fornecer cartões de identidade, a Trub presta serviços complementares, como *design* de cartão, personalização ou consultoria.

  http://www.trueb.ch/en/identity-documents/identity-trust

- Fábrica Nacional de Moneda y Timbre- Casa de la Mneda (FNMT-RCM): Empresa pública espanhola que atua na produção de e-passaportes, carteiras de

motorista e a eID da Espanha. Oferece serviços de consultoria para projetos integrais de identificação.

http://www.fnmt.es/productos-y-servicios/tarjetas-electronicas/documentos-de-identificacion/documentos-nacionales-de-identidad

3) Desenvolvedores de *software*:
   - Sistemas operacionais para *smartcards*:
     - Oracle: desenvolve a plataforma aberta Javacard para *smartcards* de baixo poder computacional para multi-aplicações, com possibilidade de adição de aplicação pós-emissão.

       http://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html

     - MAOSCO: Consórcio aberto para desenvolvimento de uma plataforma aberta MULTOS, multi-aplicação, para *smartcards*.
       http://www.multos.com/

     - ATOS: Desenvolve o CARDOS dedicado para *chips* Infineon, como o SLE66CX680p ou SLE78CFX3000P.

     - NXP: Desenvolve o Java Card OpenPlatform (JCOP), implementado originalmente pela IBM, que possui uma máquina virtual Java Card que permite o uso de aplicações escritas em Java.

     - Giesecke & Devrient: Desenvolve o STARCOS especifico para eIDs.

       http://www.gi-de.com/gd_media/media/en/documents/brochures/government_1/STARCOS-35-ID.pdf

- Gemalto: Desenvolve o Sealys MultiApp ID especifico para eIDs com várias aplicações.

  http://www.gemalto.com/govt/sealys/id_solutions/index.html

- *Middleware* para *smartcards*:
  - Charismatics: Desenvolve *middleware* para cartões PIV, PKI, entre outros.
    http://www.charismathics.com/products/middleware/cssi-piv/

  - United Access: Desenvolve *middleware* compatível com sistemas operacionais como SICRYPT, CardOS e JCOP, usando interfaces CSP e PKCS#11.
    https://www.united-access.com/smart-card-middleware

- *Match on Card*:
  - Precise: Desenvolve o MOC para verificação de impressão digital por *templates* em eID´s.
    http://www.matchoncard.com/benefits-of-moc/i-work/

  - Neurotechnology: Desenvolve o MegaMatcher On Card SDK para verificação de irís, impressão digital e face por *templates*.

    http://www.neurotechnology.com/megamatcher-on-card.html

b. No Brasil

1) Fabricantes de *chip*:

- CEITEC: Possuem fábrica em Porto Alegre - RS. Ainda não iniciou a produção em larga escala de pastilhas de silício. A perspectiva de início de fabricação é para 2016. Possuem *design-house*, mas o único projeto na área de identificação é do *chip* compatível com aplicação ICAO para passaporte eletrônico, CTC 21001.

http://www.ceitec-sa.com/pt/rfid

- SIX Semiconductors: Possuem fábrica em Ribeirão das Neves (MG). Está realizando ainda um programa mundial de recrutamento e não iniciou a produção em larga escala de pastilhas de silício. Não há nenhuma informação sobre produtos aplicáveis a eID.

http://www.sixsemicondutores.com.br/technology-and-products/#smartcards

2) Fabricantes de cartões ID-1 e integradores de tecnologia:

- GEMALTO: Possui parque de produção de cartões ID-1 em Curitiba-PR e sítio de personalização em Barueri-SP.

- Oberthur: Possui parque de produção de cartões ID-1 com smartcards em Cotia-SP, onde é produzida a eID do Perú.

- Giesecke & Devrient: Dispõe de um parque industrial em Itaquaquecetuba-SP, onde produz e personaliza cartões nas áreas de Telecomunicações, Meios de Pagamentos e Governo & Soluções, além de cartões inteligentes compatíveis com as normas ICP-Brasil para as principais Autoridades Certificadoras.

- Valid (Incard do Brasil): Possui parque em Santo André-SP para produção de cartões nas áreas de *telecom*, *smart cards* e identificação.

- Safram Morpho: Possui parque em Taubaté-SP para produção e personalização de cartões biométricos com tecnologia de policarbonato, além cartões para bancos e setor de *telecom*.

- Intelcav: Possui uma fábrica de cartões no sul do país e centros de personalização em São Paulo-SP e Belém-PA para produção de cartões bancários.

2.6 Informações sobre projetos de eID e identidades nacionais.

A Tabela 1 lista informações de sítios eletrônicos sobre eID [5], identidades nacionais e internacionais.

Tabela 1: Sítios eletrônicos sobre eID´s e identidades nacionais e internacionais.

País	Sítio Eletrônico
Áustria	www.buergerkarte.at
Bélgica	http://eid.belgium.be/
Suíça	http://www.suisseid.ch/
República Tcheca	http://www.mvcr.cz/clanek/osobni-doklady.aspx http://www.mojeid.cz/
Estônia	www.id.ee
Finlândia	http://www.fineid.fi/
Alemanha nPA	https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/EID_node.html
Itália (CNS)	CNIPA Web www.progettocns.it www.progettocns.it
Itália (CIE)	www.servizidemografici.interno.it
Lituânia	www.nsc.vrm.lt www.eid.lt www.dokumentai.lt
Espanha	www.dnielectronico.es http://www.cert.fnmt.es/ http://www.accv.es/default_default.htm http://www.izenpe.com/s15-5218/es/
Portugal	www.cartaodecidadao.pt
Holanda	https://www.digid.nl/index.php?id=1&L=1 http://www.eherkenning.nl/
Suécia	http://www.telia.se/privat/katalog/VisaProdukt.do?channelId=-76442&tabId=0&OID=1537014385&type=PRODUCT
Malásia	http://mykadpro.onlineapp.com.my/default.aspx
Turquia	www.ekds.gov.tr
Peru	http://www.reniec.gob.pe/portal/intro.htm
EUA (TWIC)	http://www.tsa.gov/stakeholders/transportation-worker-identification-credential-twic%C2%AE
EUA (PIV)	http://csrc.nist.gov/groups/SNS/piv/standards.html
SID (*Seafares Identity Document*)	http://www.ilo.org/global/standards/maritime-labour-convention/text/WCMS_162321/lang--en/index.htm

3 TÓPICOS REFERENTES A PRODUÇÃO, MODELOS DE GERENCIAMENTO, TECNOLOGIAS, E EMPREGO DE EID´S.

Na última década, um grande número de projetos de identidade nacional eletrônica foi lançado, notadamente na Europa e na Ásia. Cabe ressaltar que alguns países optaram por ainda utilizar verificação biometria por meio da gravação dos dados impressos no cartão, que não possui *chip*, como é o caso do México.

Países como Japão, EUA, Inglaterra e França ainda não desenvolveram ou não lançaram seus projetos, principalmente em virtude da preocupação da população em relação à privacidade e a rejeição à centralização de dados pessoais e biométricos pelo governo.

O foco dos modelos adotados por cada país varia muito. Alguns países priorizam aplicações de e-governo por meio da autenticação remota; alguns buscam expansão de aplicações para setor privado como bancário, meios de pagamento e transporte público; outros desenvolvem técnicas para garantia da privacidade para alcançar maior adesão da população; e outra parte prioriza simplesmente o combate à fraude ou terrorismo com base em uma autenticação forte usando biometria.

No setor industrial de produção de eID se observa uma grande evolução, com tecnologias específicas para eID, mas ainda sem uma maturação de tecnologias nem mesmo de padrões, o que dificulta a identificação clara de uma solução ótima para emprego em identidades eletrônicas.

O que se observa, portanto, é que apesar de grande número de projetos lançados, não há uma padronização de modelos de autenticação ou recursos de privacidade, tampouco de requisitos de segurança física dos *chips*, de forma que cada país adota uma solução diferente. Uma exceção a essa regra é o caso do Cartão do Cidadão de Portugal que adotou a mesma solução e modelo utilizado na eID BELPIC da Bélgica, por meio de cooperação técnica com o *Federal Public Service for Information and Communication Technology* (FEDICT-Bélgica).

Esta falta de um modelo universal tem ensejado diversos esforços no sentido de padronização, como na especificação técnica do Cartão do Cidadão Europeu (*European Citizen Card* –ECC), CEN TS 15480, pelo comitê europeu de normatização (CEN) a partir de 2007. Entretanto, devido à pequena participação dos governos nesse projeto, projetos subsequentes de eID, como o da Alemanha, não seguiram a especificação proposta. Outros esforços buscando interoperabilidade de eID´s para autenticação vem sendo

realizados como o programa STORK (*Secure Identity Across Borders Linked*) e FutureID, que também prevê uma proposta de um modelo centrado no usuário.

Dessa forma, uma análise global das diversas soluções de eID´s nos possibilita avaliar as vantagens e desvantagens de possíveis serviços e funcionalidades, adequando-as a nossa realidade, bem como adotar melhores soluções em termos de privacidade, segurança, durabilidade e custo/benefício. Nesse sentido, este estudo, inicial e não exaustivo, visa levantar informações acerca de tecnologias e modelos adotados em eID´s, para identificar diretrizes e funcionalidades desejáveis, bem como prever possíveis problemas e ameaças.

O presente relatório engloba estudo sobre modelos de eID adotados por vários países da Europa, alguns da Ásia, dos EUA, do México e de países da América do Sul com projetos já lançados, como Chile e Peru.

Com o objetivo de facilitar a comparação, a análise dos modelos é dividida por aspectos técnicos:

- Protocolos de autenticação remota e modelo de gerenciamento de eID;
- Recursos de privacidade;
- Especificação técnica do *chip* e do sistema operacional;
- Estrutura de dados, métodos de acesso a escrita e leitura;
- Personalização e inclusão de aplicações;
- Desenvolvimento e padronização do *Middleware*;
- Verificação biométrica, *Match on Card* e proteção da biometria;
- Uso e padrões de assinaturas digitais;
- Processos de fabricação, homologação e durabilidade.

Além destes aspectos tecnológicos, outros temas relacionados são cobertos pela pesquisa, como:

- projeto e emissão;
- aplicações contidas na eID;
- serviços disponibilizados e adesão da população;
- custo, local de fabricação e gerência da eID.

3.1 Projeto e emissão

(Em andamento)

3.2 Custo, local de fabricação e gerência da eID

(Em andamento)

3.3 Protocolos de autenticação remota e modelo de gerenciamento de eID

(Em andamento)

3.4 Recursos de privacidade

(Em andamento)

3.5 Uso e padrões de assinaturas digitais

(Em andamento)

3.6 Verificação biométrica, *Match on Card* e proteção da biometria

(Em andamento)

3.7 Especificações técnicas do *chip* e sistema operacional

(Em andamento)

3.8 Estrutura de dados e critérios de acesso à leitura/escrita

(Em andamento)

3.9 Personalização e inclusão de aplicações

(Em andamento)

3.10 Desenvolvimento e padronização do *Middleware*

(Em andamento)

3.11 Aplicações contidas no *chip*/cartão

(Em andamento)

3.12 Segurança a ataques e certificação

(Em andamento)

3.13 Serviços disponibilizados e adesão da população

(Em andamento)

3.14 Processos de fabricação, homologação e durabilidade

(Em andamento)

4 CONCLUSÃO

Pendente. Trabalho incompleto.

Referências

[1] W. E. Wolfgang Rankl, Smart Card Handbook, 4th Edition, Wiley, 2009.

[2] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd Edition, Wiley, 2010.

[3] M. P. Walter Fumy, Handbook of eID Security: Concepts, Practical Experiences, Technologies, Wiley, 2011.

[4] S. M. A. M. Norberto Nuno Gomes de Andrade, “Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020),” JRC Scientific and Police Reports (Europe Commission), 2013.

[5] “STORK 2.0 Member State´s eIDs,” STORK 2.0, 2013.

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br