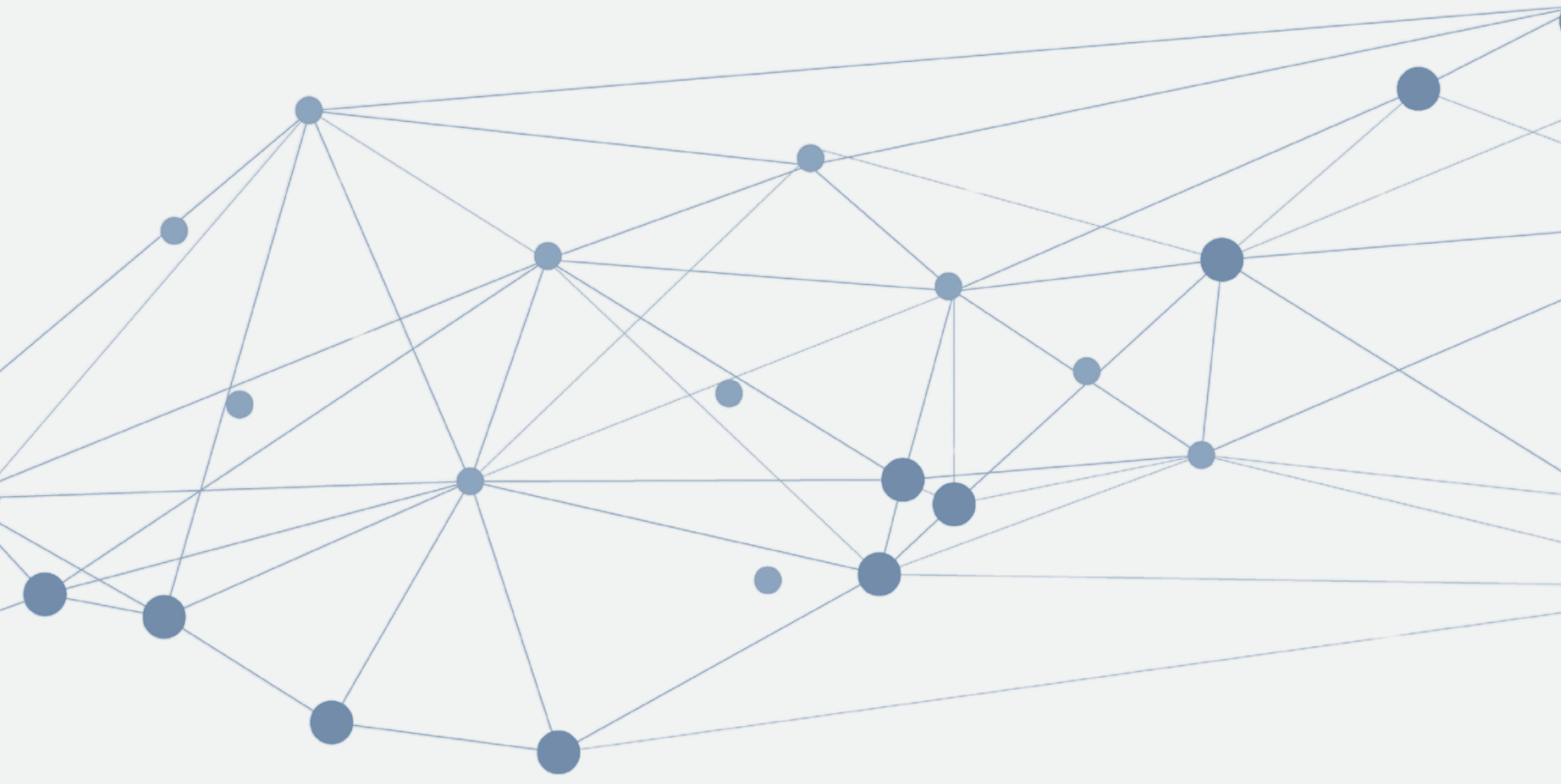
TÜBİTAK
BİLGEM

e-ID Technologies

SOLUTION CATALOG

TÜBİTAK **BİLGEM**
INFORMATICS AND INFORMATION
SECURITY RESEARCH CENTER

WE ARE AT THE HEART OF TECHNOLOGY



Our Competencies

TÜBİTAK BİLGEM has achieved many national and international successes with the technologies it has developed, the products it has produced, and the Competence Centers it has established.

BİLGEM continues to make our nation proud through the innovative solutions it provides to universities, the military, public institutions, and the private sector — supported by the robust infrastructure it builds and the strategic collaborations it fosters.

Moving forward with determination, BİLGEM strives to become an R&D center that shapes the future, making our country a leading reference in global science and technology.

TÜBİTAK BİLGEM e-ID Technologies:
Securing Digital Identity

TÜBİTAK BİLGEM is Türkiye's leading national technology center, committed to advancing high-assurance e-ID and cybersecurity solutions that strengthen the nation's technological sovereignty, resilience, and digital trust.

Leveraging decades of research excellence and deep-rooted engineering expertise, BİLGEM develops end-to-end, scalable, and secure digital identity systems that meet international standards while preserving national control over critical technologies.

Our comprehensive portfolio, powered entirely by domestic innovation and national resources, spans the entire digital identity lifecycle — from the secure chip operating system and cryptographic middleware to management, authentication, and verification infrastructures — enabling trusted, interoperable, and future-ready e-ID ecosystems.

Partnering for Progress:
e-ID Solutions for a Secure Future

Did you know that beyond adopting TÜBİTAK BİLGEM's cutting-edge technologies, your organization can also collaborate with us to develop tailored R&D solutions that meet your unique needs?

This e-ID Technologies Solution Catalog has been prepared to provide deeper insight into TÜBİTAK BİLGEM's technological expertise and to demonstrate how we can work together to shape the future of secure digital identity systems.

Together, we can strengthen trust in digital interactions, enable seamless public and private services, and support the transition to data-driven governance models. Our goal is to help institutions build the foundations of a secure, inclusive, and citizen-centric digital ecosystem.

Let's join forces to unlock the full potential of e-ID technologies — creating smarter connections, empowering individuals, and advancing societies toward a more secure digital future.

TÜBİTAK BİLGEM
Empowering Innovation. Advancing Nations.

TÜBİTAK BİLGEM
e-ID Technologies

AKİS Smart Card Operating System

- **PKI** E-ID AND E-SIGNATURE CARD
- **e-BİLET** E-TICKET, ACCESS CONTROL AND LOYALTY CARD
- **GEZGİN** E-DRIVING LICENCE, E-PASSPORT, E-ID AND E-SIGNATURE APPLICATION

EKİNOX ID Document Lifecycle Management Platform

DTC Digital Türkiye Wallet

AKiS PKI

E-ID AND E-SIGNATURE CARD

Developed in compliance with ISO/IEC 7816 standards, the AKiS PKI smart card family—comprised of AKiS v2.2, v2.5, and v2.6—provides a secure, interoperable, and reliable foundation for digital identity and electronic signature solutions.

AKiS PKI products enable strong authentication, digital signing, and secure access across various public and private sector applications. Their advanced Public Key Infrastructure (PKI) architecture supports a wide range of cryptographic algorithms and ensures high levels of security and data integrity.

With their proven performance in e-Government, corporate, and financial systems, AKiS PKI smart cards help institutions establish trusted digital identities, safeguard transactions, and build a resilient digital ecosystem aligned with global standards.

AKiS PKI

AKiS PKI

E-ID AND E-SIGNATURE CARD

FEATURES
ISO/IEC 7816-3 contact-based communication
ISO/IEC 7816-4, 8, 9 compliant APDU command set
Secure messaging with AES-256
Hash computation (SHA-1, SHA-256, SHA-384, SHA-512)[1]
Random Number Generator (RNG)[2]
Card Verifiable Certificates (CVC)[3]
Role-based access control mechanism
RSA Digital Signature Generation and Decryption[3]
RSA key pair generation[4]
ECDSA digital signature generation (ECC 128 – 640 bits)[5]
ECC key pair generation (ECC 128 – 640 bits)[5]
Cryptographic checksum computation (DES3 MAC/CMAC/RetailMAC, AES MAC/CMAC)[5]
Symmetric encryption/decryption (DES3, AES: CBC, ECB, GCM)[6]
Wrap / Unwrap Key[7]
ECDH Key Derivation[7]
Session based symmetric key generation[7]
Session based ECC key pair generation[7]
Common Criteria (CC) EAL 4+ security evaluation
Support for multiple chip platforms[8] • UKTÜM-H v7.01 • Infineon SLE78CFX2400P • NXP P71D320P, P71D352P
Support for PKCS#11[9]
Support[10] for CSP and Minidriver

[1] AKiS v2.2 supports SHA-1 and SHA-256 only.

[2] AKiS v2.2 supports true random number generation whereas AKiS v2.5 and v2.6 support Hybrid Deterministic random number generation.

[3] AKiS v2.5 supports RSA 1024 – 2816 bits and AKiS v2.6 supports RSA 1024 – 2688 bits whereas AKiS v2.2 supports RSA 1024 bits and 2048 bits only.

[4] AKiS v2.5 supports RSA 1024 – 2816 bits and AKiS v2.6 supports RSA 1024 – 2688 bits whereas AKiS v2.2 supports RSA 2048 bits only.

[5] AKiS v2.5 and v2.6 only.

[6] AKiS v2.5 and v2.6 only (block type GCM supported by AKiS v2.6 only).

[7] AKiS v2.6 only.

[8] Hardware platforms are certified for CC EAL 5+ or above.

[9] MS Windows, Linux and MacOS operating systems.

[10] MS Windows operating system only.

AKiS BiLET

E-TICKET, ACCESS CONTROL AND LOYALTY CARD

Developed by TÜBİTAK BİLGEM, AKiS BiLET is a contactless smart card solution based on OSPT CIPURSE[1] open standards. Featuring an advanced security architecture and a cost-effective design, AKiS BiLET is engineered specifically for use as an electronic payment medium in Automated Fare Collection (AFC) systems. In addition, it is the first smart card product developed in Türkiye that provides reliable contactless functionality for a range of applications, including access control and parking systems.

AKiS BiLET

AKiS BiLET

E-TICKET, ACCESS CONTROL AND LOYALTY CARD

GENERAL PROPERTIES
Contactless baud rate up to 848 kbps
Operating frequency 13,56 MHz
ISO/IEC 14443A-L4 compliance
ISO/IEC 7816 compliant file system
ISO/IEC 7816-4, 9 compliant APDU command set[2]
8 applications[2], configurable
32 files[2] per application, configurable
Support for binary and record file types
CTM (Consistent Transaction Mechanism)[3]
Multi-application support

SECURITY FEATURES
Hardware platform certified for CC EAL 6+
True Random Number Generator (TRNG)
AES-128[4] encryption algorithm
8 AES-128 keys per application
Easy and flexible key management system
Resistant to Differential Power Analysis (DPA) attacks
Resistant to Differential Fault Analysis (DFA) attacks
Mutual Authentication based on ISO/IEC 9798-2 (AES-128)
Secure messaging modes based on ISO/IEC 7816-4 (Plain, AES MACed, AES ENCed)
File based access control and secure messaging

TARGET APPLICATIONS
e-Ticket applications
Personnel attendance control systems
Access control systems
Car parks
Libraries
Health card, social card and loyalty applications

CIPURSE OPEN SPECIFICATIONS

CIPURSE open specifications provide a proven technology based on ISO/IEC 7816, ISO/IEC 14443 standards and Advanced Encryption Standard (AES) to offer secure, flexible and standard automatic fare collection systems.

INDEPENDENT TECHNOLOGY

Platform independent: CIPURSE technology can be implemented either as a native application on smart card chips or as applets on Java Cards.

Vendor independent: CIPURSE technology is not a proprietary solution of a particular company: it is an open standard and open technology product that can be implemented by any company. Today, several technology companies including TÜBİTAK BİLGEM have certified CIPURSE products and the number of such companies are increasing day by day.

Card reader independent: CIPURSE technology does not require any special hardware for communication: any card reader conforming to ISO/IEC 14443A-L4 standards can be used with CIPURSE cards.

[1] CIPURSE open specifications are published by OSPT Alliance. TÜBİTAK BİLGEM is a full member of OSPT Alliance.

[2] CIPURSE T Profile only.

[3] CTM is a mechanism used to avoid inconsistent update of data stored on the card.

[4] AES Advanced Encryption Standard, ISO/IEC 18033- 3, FIPS 197.

AKiS GEZGiN

e-PASSPORT

with e-ID and e-SIGNATURE APPLICATIONS

AKiS GEZGiN e-Passport application is compatible with ICAO Doc 9303 standards. The information stored on contactless chip can only be accessed via secure communication protocols such as Basic Access Control (BAC) and Supplemental Access Control (SAC). Active Authentication (AA) and Chip Authentication (EAC - CA) prevent cloning of the e-Passport. In addition, biometric data on the chip is protected by Extended Access Control (EAC) and CVC certificates. Therefore, only those countries that are allowed by the issuing country can access the biometric data.

AKiS GEZGiN extends ICAO Doc 9303 standards by increasing the number of supported roles to 32 and it also supports e-Signature applications. Therefore, it can also be personalized for e-ID and/or e-Signature applications.

AKiS GEZGiN

E-PASSPORT, E-ID AND E-SIGNATURE APPLICATION

FEATURES
ICAO LDS 1.7[1]
Basic Access Control (BAC)
Active Authentication (AA) RSA (up to 2560 bits)[2] SHA-1, SHA-256, SHA-384, SHA-512 ECC (up to 521 bits): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Supplemental Access Control (SAC) PACE v2 Support for MRZ, CAN and PIN[3] Support for Generic Mapping and Integrated Mapping ECDH (Brainpool curves up to 512 bits) DH (1024 bits, 2048 bits)
Extended Access Control (EAC) EAC v1[4] RSA (up to 3072 bits): SHA-1, SHA-256, SHA-512 ECC (up to 521 bits): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Contactless communication ISO/IEC 14443-3, 4 Type A Baud rate: 424/848 kbps
Secure messaging DES3 AES-128, AES-192, AES-256
Common Criteria (CC) security evaluation CC EAL 4+ (ALC_DVS.2) for BAC CC EAL 5+ (ALC_DVS.2, AVA_VAN.5) for SAC & EAC
Multiple chip platforms[5] Infineon[6] SLE78CLFX3000P, SLE78CLFX308AP, SL78CLFX4000P, SLE78CLFX408AP NXP P71D320P[6], P71D352P[7]
Compliance with standards ICAO Doc 9303 ISO/IEC 14443-3, 4 ISO/IEC 7816-4, 8, 9 ICAO Technical Report Supplemental Access Control for MRTDs BSI TR-03110 BSI TR-03111

[1] AKiS GEZGiN v2.0 supports more data groups than defined by ICAO.

[2] Maximum supported RSA bit length for AKiS GEZGiN v1.x is 2048 bits.

[3] Support for PINs is available only for AKiS GEZGiN v2.0.

[4] AKiS GEZGiN v2.0 supports a maximum of 32 roles.

[5] Hardware platforms are certified for CC EAL 6+.

[6] AKiS GEZGiN v1.x only.

[7] AKiS GEZGiN v2.0 only.

BASIC ACCESS CONTROL (BAC)

Basic Access Control (BAC) is a mechanism used in e-Passports to prevent chip skimming and eavesdropping on the communication between e-Passports and the terminals by encrypting the transmitted information. BAC ensures that only authorized terminals can read information from e-Passports: before any data can be read, the terminal needs to prove that it has physical access to e-Passport by using a session key derived from the Machine Readable Zone (MRZ) or Card Access Number (CAN).

SUPPLEMENTAL ACCESS CONTROL (SAC)

SAC, a mechanism based on Diffie-Hellman key exchange protocols (DH/ECDH), provides securer and stronger session keys than BAC. For the e-Passport use case, where the passport holder is automatically assumed to have agreed to their on-chip non-biometric data to be accessed by terminals when they hand in their passport, SAC with MRZ/CAN can be used. However, for other use cases such as e-ID and e-Signature, where the cardholder is expected to be authenticated before cryptographic services or on-chip non-biometric data are accessed, SAC with PIN can be used.

EXTENDED ACCESS CONTROL (EAC)

EAC is a mechanism that enhances the security features of e-Passports by adding functionality to check the authenticity of both the chip (via Chip Authentication – CA) and the terminals (via Terminal Authentication – TA): EAC CA updates secure messaging session keys with stronger session keys and EAC TA uses role-based CVC certificates to ensure that only authorized terminals can read optional biometric data groups (DG3 and DG4) from e-Passports. For the e-ID use case, AKiS GEZGiN increases the number of supported roles to 32; therefore, more files (EFs) than required by EAC can be protected by role authentication.

ACTIVE AUTHENTICATION (AA)

Active Authentication prevents cloning of the chip.

AKiS GEZGiN

e-DRIVING LICENCE

with e-ID and e-SIGNATURE APPLICATIONS

AKiS GEZGiN e-Driving Licence (ISO-compliant Driving Licence - IDL) application is compatible with ISO/IEC 18013 standards. The information stored on the contactless chip can only be accessed via secure communication protocols such as Basic Access Protection (BAP) and Supplemental Access Control (SAC). Active Authentication (AA) and Chip Authentication (EAC – CA) prevent cloning of the e-Driving Licence. In addition, biometric data on the chip is protected by Extended Access Control (EAC) and CVC certificates. Therefore, only those countries that are allowed by the issuing country can access the biometric data.

AKiS GEZGiN extends ISO/IEC 18013 standards by increasing the number of supported roles to 32 and it also supports e-Signature applications. Therefore, it can also be personalized for e-ID and/or e-Signature applications.

AKiS GEZGiN

AKiS GEZGiN

E-DRIVING LICENCE, E-ID AND E-SIGNATURE APPLICATION

FEATURES
ISO/IEC 18013-2 LDS[1]
Basic Access Protection (BAP)
Active Authentication (AA) RSA (up to 2560 bits)[2]: SHA-1, SHA-256, SHA-384, SHA-512 ECC (up to 521 bits): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Supplemental Access Control (SAC) PACE v2 Support for SAI and PIN[3] Support for Generic Mapping ECDH (Brainpool curves up to 512 bits)
Extended Access Control (EAC) EAC v1[4] ECC (up to 521 bits): SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Contactless communication ISO/IEC 14443-3, 4 Type A Baud rate: 424/848 kbps
Secure messaging DES3 AES-128, AES-192, AES-256
Common Criteria (CC) security evaluation[5] CC EAL 4+ (ALC_DVS.2) for BAP CC EAL 5+ (ALC_DVS.2, AVA_VAN.5) for SAC & EAC
Support for multiple chip platforms[6] Infineon[7] SLE78CLFX3000P, SLE78CLFX308AP, SLE78CLFX4000P, SLE78CLFX408AP NXP P71D320P[7], P71D352P[8]
Compliance with standards ISO/IEC 18013-3 ISO/IEC 14443-3, 4 ISO/IEC 7816-4, 8, 9 ICAO Technical Report Supplemental Access Control for MRTDs BSI TR-03110 BSI TR 03111

[1] AKiS GEZGiN v2.0 supports more data groups than defined by ISO/IEC 18013.

[2] Maximum supported RSA bit length for AKiS GEZGiN v1.x is 2048 bits.

[3] Support for PINs is available only for AKiS GEZGiN v2.0.

[4] AKiS GEZGiN v2.0 supports a maximum of 32 roles.

[5] Common Criteria (CC) certification is available for AKiS GEZGiN v2.0 only.

[6] Hardware platforms are certified for CC EAL 6+.

[7] AKİS GEZGİN v1.x only.

[8] AKİS GEZGİN v2.0 only.

BASIC ACCESS PROTECTION (BAP)

Basic Access Protection (BAP) is a mechanism used in e-Driving Licences to prevent chip skimming and eavesdropping on the communication between e-Driving Licences and the terminals by encrypting the transmitted information. BAP ensures that only authorized terminals can read information from e-Driving Licences: before any data can be read, the terminal needs to prove that it has physical access to e-Driving Licence by using a session key derived from the SAI (Scanning Area Identifier).

SUPPLEMENTAL ACCESS CONTROL (SAC)

SAC, a mechanism based on Diffie-Hellman key exchange protocol (ECDH), provides securer and stronger session keys than BAP. For the e-Driving Licence use case, where the licence holder is automatically assumed to have agreed to their on-chip non-biometric data to be accessed by terminals when they hand in their licence, SAC with Scanning Area Identifier (SAI) can be used. However, for other use cases such as e-ID and e-Signature, where the cardholder is expected to be authenticated before cryptographic services or on-chip non-biometric data are accessed, SAC with PIN can be used.

EXTENDED ACCESS CONTROL (EAC)

EAC is a mechanism that enhances the security features of e-Driving Licences by adding functionality to check the authenticity of both the chip (via Chip Authentication – CA) and the terminals (via Terminal Authentication – TA): EAC CA updates secure messaging session keys with stronger session keys and EAC TA uses role-based CVC certificates to ensure that only authorized terminals can read optional biometric data groups (DG7 and DG8) from e-Driving Licences. For the e-ID use case, AKiS GEZGiN increases the number of supported roles to 32; therefore, more files (EFs) than required by EAC can be protected by role authentication.

ACTIVE AUTHENTICATION (AA)

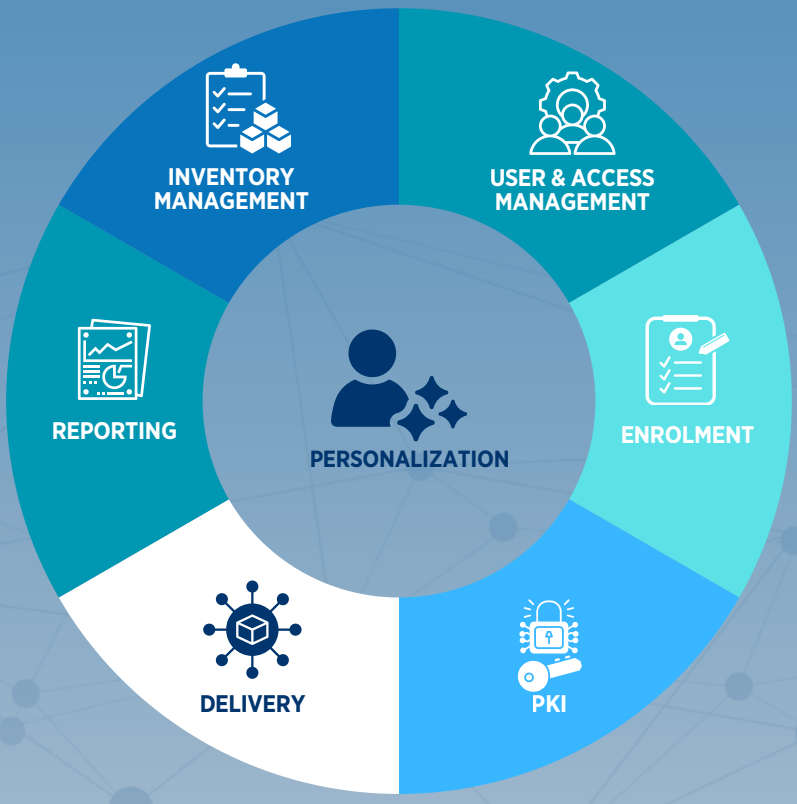
Active Authentication prevents cloning of the chip.

EKİNOX

ID DOCUMENT LIFECYCLE MANAGEMENT PLATFORM

Modern identity management is no longer just a document production process — it is an experience where trust, speed, and integrity converge.

Our Identity Document Lifecycle Management Application enables you to manage the entire lifecycle of all identity documents — from e-Passports to e-Driver's Licenses, from e-Signatures to personalized e-ID cards — through a single unified platform.



SECURE, FLEXIBLE AND SCALABLE

ekinox

EKİNOKS

ID DOCUMENT LIFECYCLE MANAGEMENT PLATFORM

WHY CHOOSE US?

Modular Design: Web-based microservice architecture providing flexible, customer-specific configurations with low maintenance costs.

High Security: Full compliance with international standards (ICAO, BSI, EAC).

Fully Integrated: Seamless connectivity with AFIS/ABIS, PKI, HSM, LDAP, OpenID, BI tools, and more.

Real-Time Traceability: End-to-end monitoring and control over enrolment, inventory management, personalization, and delivery processes.

SUPPORTED DOCUMENT TYPES

- e-Passports
- National e-ID Card
- e-Drivers Licenses
- Residence Permit Cards
- Firearm Licenses
- Electronic Signature Card
- Access Cards
- Customer-Specific ID Documents

and more...

PKI AND CRYPTOGRAPHIC SECURITY

CVCA, CSCA, DS, DV profiles compliant with BSI TR-03110 and ICAO 9303.

HSM-based key generation, secured storage, and usage.

Authorized terminal access using Terminal Authentication (TA) and Extended Access Control (EAC) mechanisms.

High-security digital signature and authentication using RSA and ECDSA algorithms.

REFERENCE PROJECTS

Republic of Türkiye National e-ID Card Project

Turkish Republic of Northern Cyprus National e-ID Card Project

Republic of Türkiye e-Passport Project

Republic of Türkiye e-Driver's License Project

Multiple Secure Access Control Systems across the market

Residence Permit, Firearm License, and Private Security Card Solutions

SYSTEM MODULES

Appointment Management Module

- Centralized scheduling and management of enrolment appointments.
- Real-time coordination between registration offices and personalization centers.

Application Management Module

- Secure collection of applications via web or mobile platforms, in full compliance with ICAO standards
- Accurate capture of biometric data through AFIS/ABIS integration
- Enhanced user experience with real-time application status tracking

Personalization Module

- Batch-based industrial production and document personalization.
- ICAO-compliant data encoding and visual personalization.
- Automatic quality inspection and chip verification.
- Complete PIN/PUK management.
- Full integration with desktop and industrialprinters/card personalization machines.
- Customizable surface designs per customer specification.
- Comprehensive audit logs of all personalization operations.

Secure Inventory Management Module

- Tracking of serialized and non-serialized blank documents.
- e-Signature-based inventory management.
- Role-based access control and approval workflows.
- Waste tracking and secure delivery chain.
- Complete inventory audit trail.

Reporting Module

- Dynamic, customizable, filterable data visualization and analytics.
- Report export various formats such as PDF, Excel, and Word.
- Integration with Business Intelligence tools.
- Real-time operational and performance dashboards.

Enveloping Module (Optional)

- Integration with high-speed enveloping and dispatch systems.
- Customer-specific delivery management and shipment tracking.

User and Access Management Module

- Centralized user and role administration.
- Role-based access control (RBAC) with operation-level permissions.
- LDAP and OpenID compatibility.
- Full user activity logging and traceability.

DTC

DIGITAL TÜRKİYE WALLET

The Digital Türkiye Wallet (DTC), developed under the leadership of TÜBİTAK BİLGEM, represents a milestone in Türkiye's digital transformation journey — a secure, user-centric platform designed to unify public, private, and international digital services. By enabling citizens and organizations to manage and verify their identities through a single trusted wallet, DTC empowers individuals to interact seamlessly across sectors and borders. Built upon the principles of sovereignty, trust, and interoperability, it advances Türkiye's goal of becoming a globally recognized digital nation.

Engineered with privacy-by-design architecture and cutting-edge authentication technologies, DTC ensures that users retain full control over their personal data. Sensitive information is stored securely on the device, protected through biometric or PIN-based verification, and shared selectively based on user consent. From accessing government services to opening a bank account abroad, DTC enables frictionless, passwordless, and secure digital interactions — redefining how identity and trust are managed in the modern world.

DTC

DTC
DIGITAL TÜRKİYE WALLET

FEATURES

User Management: Users determine the data they wish to share (e.g., age, driver's license, diploma). Through selective disclosure, only required information is communicated.

Privacy and Security: Data is stored locally on the device (e.g. eSIM-based wallet), thereby preventing tracking or profiling.

Portability: Identity documents can be utilized across a range of services within the Republic of Türkiye. For instance, a Turkish citizen may open a bank account in Germany using a DTC.

Accessibility: Digital documents, including identification cards, diplomas, health records, and tickets can be stored and shared.

Passwordless Authentication: Access is granted through a PIN or biometric security measures, such as fingerprint recognition, thereby mitigating phishing risks.

APPLICATIONS

Public Administration and Governance
Reconceptualize Bureaucracy

Finance and Commerce
Transact Securely

Health and Education
Safeguard Personal Information, Shape the Future

Technology and Lifestyle
A World That is Connected and Free

HOW IT WORKS
Simple, secure and intuitive.

1	**Download the Application** Download the DTC Wallet application on your device via the App Store or Google Play.
2	**Define Your Identity** Scan your chip ID using NFC or confirm your account through e-Government verification.
3	**Manage Your Information** You determine the information you disclose to each institution. Selective disclosure guarantees that only essential information is shared.
4	**Finalize Your Transaction** Your bank, university, municipality, or international transactions are executed securely within seconds.

PUBLIC ADMINISTRATION AND GOVERNANCE
Reconceptualize Bureaucracy

Legislation & Electoral Processes	Identity verification in notarial transactions (e.g. power of attorney); evidence of "Turkish citizenship and age over 18" for voter registration.
Municipal Services	ZKP-based authentication for water bill payments or access to municipal services.
Taxation and Social Services	Proof of "taxpayer" for tax returns; verification of "eligibility" for social assistance applications.

FINANCE AND COMMERCE
Transact Securely

Banking & Credit	Proof of "eligible income" or "sufficient credit score". Verification of "Turkish citizenship" when opening a bank account.
Insurance	Proof of no accident history Health insurance Data transfer between insurers
E-Commerce and Customer Loyalty	Payment authorization for online purchases Transfer of loyalty points "Over 18" age status confirmation
Telecom	Proof of citizenship Secure identity sharing Identity verification

HEALTH AND EDUCATION
Safeguard Personal Information, Shape the Future

Education & Professional Development	Diploma authenticity verification Certificate dissemination Blockchain administration of educational resources in initiatives such as BLUEDU.
Health Coverage	Verification of "Insured" status using ZKP (Zero Knowledge Proof).
Healthcare Services	Proof of vaccination Patient ID provisioning with ZKP Disclosure of blood type or allergy information in emergencies; Identity verification in medical services.

TECHNOLOGY AND LIFESTYLE
A World That is Connected and Free

Transportation and Automotive Industries

Tourism and Travel

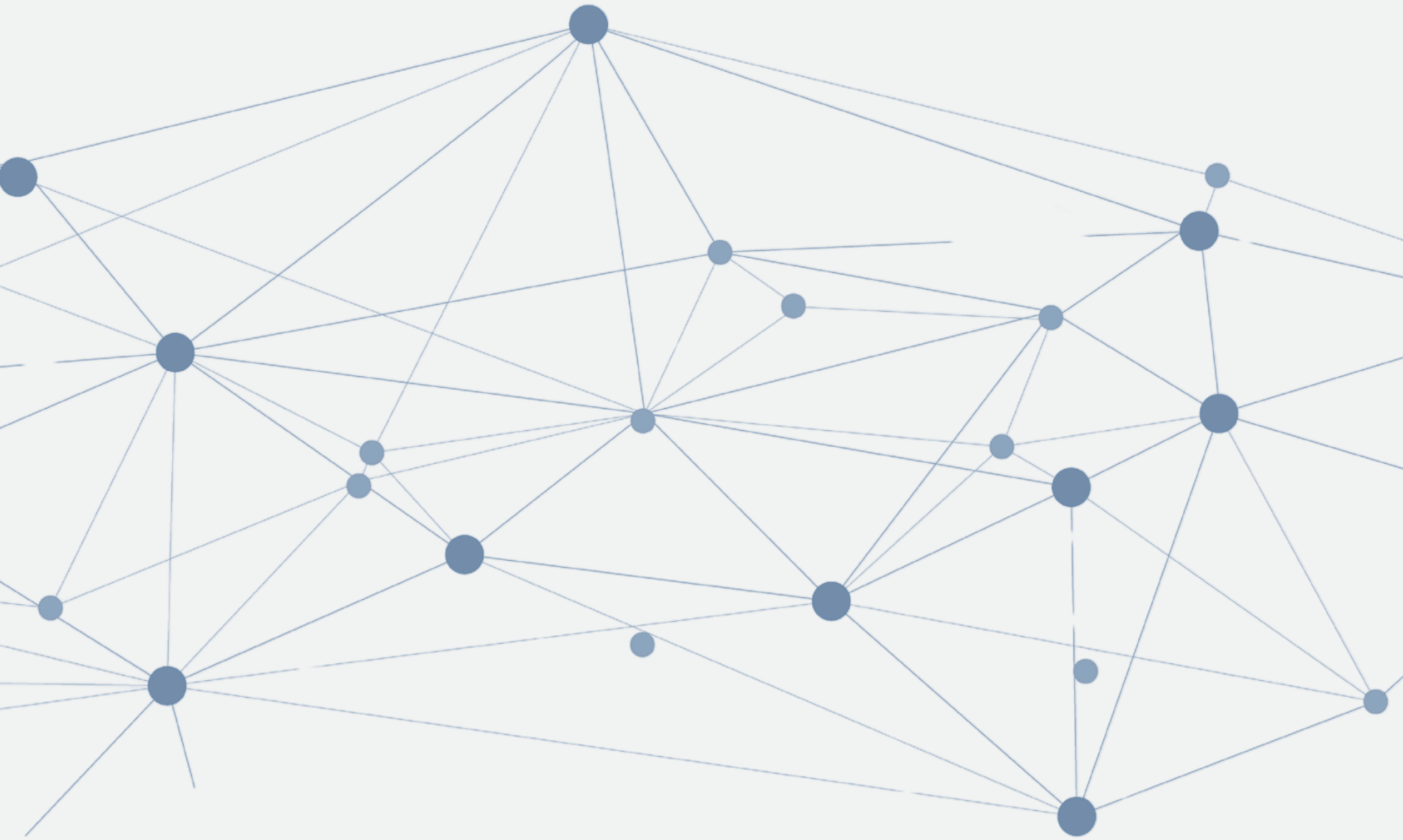
Intelligent Devices and the Internet of Things

Corporate and Supply Chain Management

Recreation and Entertainment

Energy and Agriculture

WE ARE
AT THE HEART
OF TECHNOLOGY



TÜBiTAK BiLGEM e-ID Technologies
T: +90 262 648 1000 • E: bilgem@tubitak.gov.tr
W: bilgem.tubitak.gov.tr • A: PO.: 74, 41470, Gebze, Kocaeli TÜRKİYE