SYNTIZEN®
An M2P Company

Solution Brief – Syntizen Technologies

About Syntizen Technologies

Syntizen Technologies Private Limited was founded in 2014 as a startup incubated at India's biggest Government backed Startup incubator, and member of India Stack and part of NASSCOM 10K Startups. Syntizen enables Seamless identity check that results in Delightful customer onboarding for Corporates by working with startups, middle-market businesses, state governments and other corporate companies developing innovative solutions that makes a great impact.

TSP/Solution Integrator for AUA/KUA Licensed entities

AUA/KUA is used for certain regulated entities with an Aadhaar AUA/KUA license. For licensed entities, Aadhaar returns Name, Gender, Date of Birth, Address, and Photograph to respond to e-KYC. Syntizen is a TSP/ Solution Integrator for Seamless identity check for delightful customer onboarding for corporates and efficient service delivery for governments and helps them out additionally with compliance.

Syntizen offers service to clients who are looking to onboard their customers digitally by using AUA/KUA Authentication service for verifying the status of their identity. Syntizen's AUA/KUA Solution enables collection of inputs from the customer, packaging of the collected information in the format specified by UIDAI, transfer of requests & collect responses from UIDAI, facilitate secure storage of received information and relevant logs, and transfer of relevant information to the end user. Apart from the standard functionality, Syntizen's AUA/KUA Solution provides clients with Additional Features and Services for better and efficient project handling.

Features of AUA/KUA solution

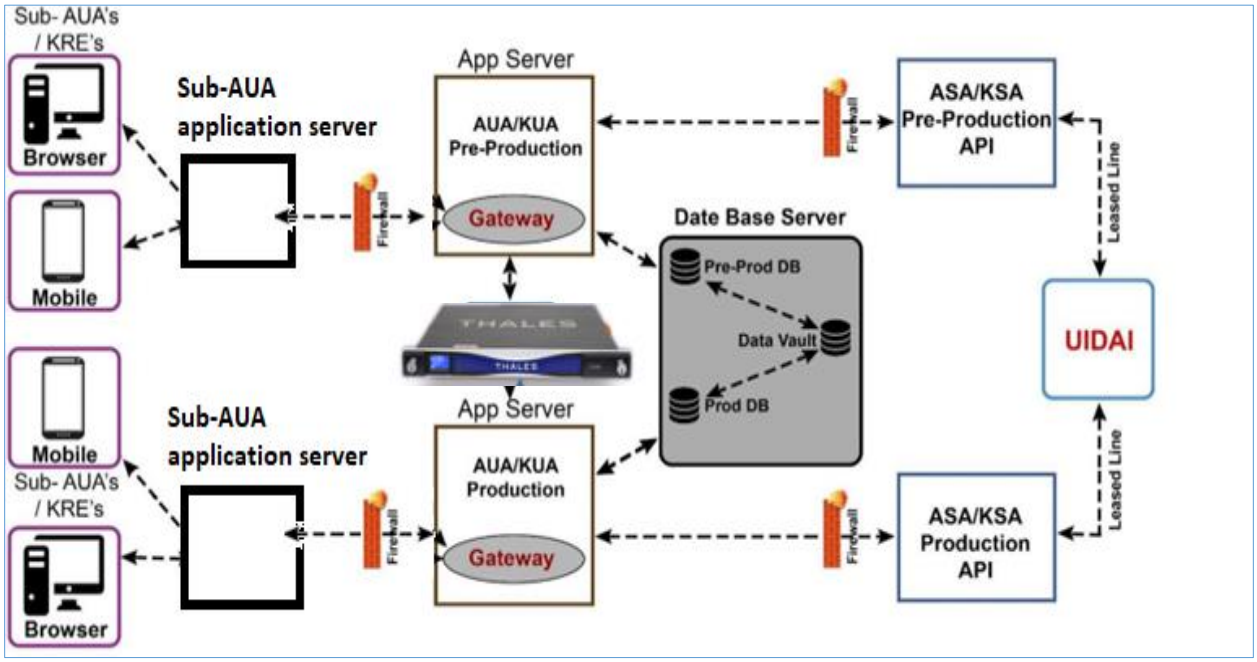
- Applying as AUA/KUA under UIDAI along with documentation support
- Performing UIDAI Test Cases for AUA & KUA in pre-production
- Integration of all STQC Certified & UIDAI Approved biometric scanners
- HSM configuration
- Data Vault Integration
- Support switching between multiple ASA's
- Maintenance of core Engine as per UIDAI guidelines
- Digital Signature Certificate (File-based Signing and Encryption)
- Support in performing CERT-IN CISA Audit as per UIDAI guidelines
- Provide sample applications for Web/Win/Android
- Provide gateway page for integration in 3rd party applications
- Admin portal

VERIFIED SOLUTION
THALES

Uniqueness of the solution

- Robust & Scalable Core engine - Core Engine is capable of handling any number of transactions & the upgrade based on transaction count can be done in minutes.
- Easy Integration & Hardware Independent - Integrate any UIDAI approved, STQC Certified devices within minutes with the help of our UIDAI SME Team.
- Live Dashboard Monitoring - Monitor every transaction, their route to UIDAI, and transaction time and error message with our Live Tracking system.
- Network Operations Center (NOC) - Unique system that keeps track of every transaction as per UIDAI and Regulator Compliance.
- Managed & Private Cloud Hosting - Manage Infrastructure i.e., Servers, HSM, etc., as per UIDAI Compliance on a time-to-time basis.
- UID Compliance Assured - Get all the UIDAI upgradations (technical & operational) within the timeline provided by UIDAI.

Architectural Diagram



Clients onboarded as AUA/KUA licensed entities, need to comply with HSM for encryption and decryption of sensitive data. During this process clients need HSM as part of the compliance for protection and prevention of loss of sensitive data. Thales will come in to help them out with a solution that can be readily integrated for protecting their sensitive data. Hence, Syntizen and Thales can work together for a better and instant onboarding experience for the client. LUNA HSM is used for our clients currently.

Mandatory use of an HSM for UIDAI

Due to the fact that the UIDs contain Personally Identifiable Information (PII), the UIDAI has mandated that the private cryptographic keys used to digitally sign and authenticate the UIDs must be stored in a Hardware Security Module (HSM) as of August 2017, and used as follows:

- Store the private keys used for digital signing of Auth XML and decryption of electronic "know your customers" (e-KYC) data
- Authentication User Agencies (AUA) and Know Your Customers User Agencies (KUA) must digitally sign the authentication requests and / or they must be signed by the Authentication Service Agency (ASA) HSM
- To decrypt the e-KYC response data received from the UIDAI, the KUA must use its own HSM
- The HSM to be used for signing Auth XML as well as for e-KYC decryption should be FIPS 140-2 compliant.

Benefits of Thales Luna HSMs

Easily conform to UIDAI mandates with Thales Luna HSMs. Ensure your data is safe from a cyber attack by storing your private cryptography keys inside a hardened, tamper-resistant, FIPS-validated device. Without access to the keys, data is rendered useless. Your organization will benefit from our years of experience, and stringent product verification testing that certifies the security and integrity of our devices.

What makes Thales HSMs the best option?

- Keys always remain in tamper-resistant hardware – protected at all times unlike alternative HSMs that store keys in software
- Secure your sensitive UID cryptographic keys in our FIPS 140-2 Level 3-validated HSMs
- Benefit from high performance to satisfy your UIDAI applications and meet service level agreements
- Strong Authentication and Access - application Private Keys remain secure from access in case of a breach
- Flexibility through broad API support as well as an unparalleled combination of products and features
- Audit logging and reporting – reduces audit and compliance

Not all HSMs are created equal

Thales takes a keys-in-hardware approach to manage and store encryption keys, unlike other HSM solutions that store keys in software. With Luna HSMs, your UIDAI private keys are protected at all times in a hardware root of trust:

- Secure your sensitive UID cryptographic keys in FIPS 140-2 Level 3–validated HSMs
- Store your private keys in a high-assurance vault to ensure they are safe from breach
- Keys never leave the HSM - applications communicate via client with keys stored in the Luna HSM

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.