

National Automotive Service Task Force Vehicle Security Committee

LSID Registry & Secure Data Release Model Terms and Conditions of Use

1.1.	<i>Preamble, Purpose & Definitions</i>	2
1.2.	<i>Policy</i>	3
1.3.	<i>Procedures</i>	7

ATTACHMENTS:

Attachment A - CONTACT INFORMATION

Attachment B - REGISTRY DENIAL AND DISPUTE RESOLUTION APPEAL PROCESS

Attachment C - APPLICATION PROCESS FOR THE NASTF REGISTRY

1.1. Preamble, Purpose & Definitions

- 1.1.1. The work and intent of the **National Automotive Service Task Force**, hereafter referred to as “**NASTF**”, and the **Vehicle Security Committee**, hereafter referred to as “**VSC**”, is to provide secure access to security related service information, including key codes, immobilizer reset information, security Personal Identification Numbers (PINs) and other information necessary needed to successfully enter, start and operate automobiles and light trucks at the request of retail consumers.
- 1.1.2. The Vehicle Security Professional Registry, hereafter referred to as “**the Registry**” and Secure Data Release Model, hereafter referred to as “**SDRM**”, gives automakers a flexible system to support 24/7 access to vehicle security information for pre-approved locksmiths and technicians. It allows aftermarket service providers to support consumer needs without undermining the integrity and basic purpose of the vehicle security systems.
- 1.1.3. This secure access to security related service information can include, but is not limited to, mechanical key codes, electronic key codes, immobilizer reset codes, PIN codes, immobilizer seed and key system information, radio lockout codes, remote codes, and successor technologies.
- 1.1.4. For the purposes of this document, automobile and light truck manufacturers will be collectively referred to as “**automakers**”.
- 1.1.5. For purposes of “the Registry” and “SDRM”, automobiles are defined as passenger vehicles and light trucks are defined as pickup trucks, vans and other light duty vehicles, excluding housecars, motor homes, motorcycles or other two-wheeled motor vehicles.
- 1.1.6. “The Registry” has been established in cooperation with participating automakers to facilitate the availability of security related service information to Vehicle Service Providers, hereafter referred to as “**VSP**”s, to support automotive consumers.
- 1.1.7. Once accepted into “the Registry”, every “VSP” will be assigned a unique Locksmith Identification number, referred to hereafter as “**LSID**”

1.2. Policy

- 1.2.1. Under the “SDRM”, security related service information is typically obtained directly from participating automakers through internet websites, telephone call centers and/or similar successor technologies. Automakers may require individual registration, subscriptions, and/or use fees and adherence to its own terms and conditions for use of/access to the websites or call centers.
- 1.2.2. To gain access to security related service information from participating automakers, all users must be pre-validated by enrolling in “the Registry” and undergoing a criminal background check process.
- 1.2.3. “The Registry” is maintained by a registry administrator appointed by NASTF (the “Registry Administrator”), which is currently the **Associated Locksmiths of America (ALOA)**, and supported by **Automotive Service Association (ASA)**. These two trade associations that represent independent automotive locksmiths and general repair shop owners respectively, oversee “the Registry” on behalf of “NASTF”. Contact information is identified in *Attachment A – Contact Information*.
- 1.2.4. “The Registry” is only available for use by businesses (sole proprietorships, partnerships and corporations) that have a taxpayer identification number and are properly licensed (where applicable) and in good standing in the jurisdictions where they conduct business. The business must provide its tax identification number with an LSID application.
- 1.2.5. Registry account types: registered LSID account holders fall into two categories, “Primary” and “Subordinate”.
 - 1.2.5.1. The Primary LSID account holder is typically, but not required to be, the business owner. The Primary LSID account holder will be required to register individually, along with his or her business.
 - 1.2.5.2. The Primary LSID account holder is responsible for all transactions and registry activity that occur on the business’ account.
 - 1.2.5.3. The Primary LSID account holder may:
 - 1.2.5.3.1. Add and remove Subordinate VSPs
 - 1.2.5.3.2. Change account access permissions for a “Subordinate”
 - 1.2.5.3.3. Manage account information for the business (phone numbers, addresses, e-mail addresses, etc)
 - 1.2.5.4. The Primary LSID account holder is responsible for all transactions that occur by Subordinate account holders.

- 1.2.5.5. Subordinate LSID account holders may manage their own passwords, but have no other administrative rights with respect to account management
- 1.2.6. Business ID: when a business account is first opened with “the Registry”, a business account number or “Business ID” is issued
- 1.2.7. Locksmith ID or LSID number: once accepted into “the Registry”, every LSID account holder, Primary and Subordinate, is assigned their own unique **LSID** that is associated with the business they registered under.
- 1.2.8. Subordinate LSID account holders also require background checks.

 - 1.2.8.1. The Primary VSP account holder is responsible to perform, or have performed by a reliable third party, a background check on all Subordinate LSID account applicants.
 - 1.2.8.2. Background checks for Subordinate LSID account applicants shall be performed to the same standards, using the same or comparable background check resources as “the Registry.”
- 1.2.9. Subcontractors: A business using “the Registry” shall not provide vehicle security information acquired through use of “the Registry” to a subcontractor or an independent contractor (as determined in accordance with the Internal Revenue Code and related rules and regulations).

 - 1.2.9.1. A business using “the Registry” (Business A) may use subcontractors and / or independent contractors who are also registered LSID account holders under a different business account (Business B), however, Business B must acquire their vehicle security information under their own LSID business account.
- 1.2.10. Expiration of LSID account: an LSID account is valid for two years

 - 1.2.10.1. Prior to account expiration, a new application must be submitted along with the appropriate fees and other information as indicated on the Registry website; adequate time must be provided for application validation and new background check to avoid gaps in information accessibility.
 - 1.2.10.2. When a Primary LSID account holder’s account expires, the accounts of all Subordinate LSIDs are locked until the primary account is revalidated.
 - 1.2.10.3. If any of the requirements for an LSID account change status during the two year term of registration (i.e. expiration of insurance, fidelity bond, termination of a business entity), it is the responsibility of the Primary LSID account holder to renew and/or update such information and notify “the Registry” within a reasonable amount of time, not to exceed 10 days.

1.2.11. Conditions of access and use of information acquired through “the Registry”:
security related service information acquired through use of “the Registry” is acquired by an LSID account holder for the direct and primary benefit of the registered vehicle owner and is provided under the condition that the LSID account holder follow all conditions of the “Positive Identification Policy” defined in *Attachment D*.

1.2.11.1. All security related information acquired on behalf of the consumer shall be promptly turned over to the consumer and then promptly destroyed by the LSID account holder. It is a violation of the terms of Registry use for an LSID account holder to retain any security related information after a transaction has been completed with the consumer.

1.2.11.2. Security related service information acquired through use of “the Registry” shall not be sold, bought, traded, bartered or shared in any way with any individual, business, entity, or person(s) other than the registered vehicle owner, except as follows:

1.2.11.2.1. Mechanical key codes may be processed through a third party, by the LSID account holder, for the express purpose of gaining the specific physical key cutting specifications (biting information to physically cut the key); the associated vehicle identification number must not be provided to the third party.

1.2.11.2.2. Once the biting information is acquired, the physical production of the mechanical key from code (code cutting, duplicating the depth and space, milling or duplicating the cut configuration, or any other method or processes) shall only be conducted by the initial LSID account holder in the presence of, or with knowledge of, the registered vehicle owner.

1.2.12. Violations of Registry terms of use: any LSID account holders who is aware of any misuse of the Registry shall immediately report said misuse directly to “NASTF LSID Registry” by contacting the NASTF Director (as identified in Attachment A – *Contact Information*).

1.2.12.1. Upon investigation and verification of misuse, the LSID account holder may be removed from “the Registry” and may be permanently restricted from being issued any subsequent LSID number/account.

1.2.12.2. Failure to report known misuse of the Registry constitutes violation of the Terms and Conditions of use of the Registry. “Failure to report” may result in removal from the Registry and permanent restriction from being issued any subsequent LSID number/account.

1.2.12.3. Sharing of user names and passwords between individuals is expressly prohibited. Breach of this policy will result in action against the LSID business owner, including potential removal from the Registry and permanent restriction from being issued any subsequent LSID number/account.

1.3. Procedures

- 1.3.1. To enroll in “the Registry”, a VSP/business must submit the following:
- 1.3.1.1. Completed and properly signed and notarized Registry Application and User Agreement (see Attachment E -- *Registry Application and User Agreement*).
 - 1.3.1.2. All applicable supporting documents and fees
 - 1.3.1.3. Federal Employer Identification Number, where applicable, and/or Social Security Number.
 - 1.3.1.4. Valid (unexpired) copy of all required Federal, State, County, and/or local governmental licenses, as required by local jurisdictions where the VSP plans to do business
 - 1.3.1.5. Valid (unexpired) copy of all required Trade Licenses and/or Business Permits, as required by local jurisdiction, where applicable.
 - 1.3.1.6. Copy of Federal 941 Quarterly Report, Federal W-2 Statement, or State recognized payroll document that lists employees, for all employees that are to be registered as LSID account holders having access to the Registry.
 - 1.3.1.7. A copy of required fidelity bond and liability insurance policies.
- 1.3.2. During the application process, all Primary LSID account applicants shall submit all information required to successfully complete a criminal background check, along with their signed and notarized application, to “the Registry” for processing.
- 1.3.2.1. An LSID applicant will be background checked as per the procedures and to the standards established in Attachment C – *Application Process for the NASTF Registry*.
 - 1.3.2.2. A felony or equivalent criminal conviction may exclude an applicant. All denied applications can be referred to the SRC for review, at the request of the applicant (see Attachment B – *Registry Denial and Dispute Resolution Appeal Process*).
 - 1.3.2.3. A Primary LSID account holder may enroll additional “Subordinate” employees in “the Registry” by performing background checks on subordinate candidates, ensuring that these individuals are covered by applicable bonds and insurance policies and following the subordinate enrollment procedures in Attachment C - *Application Process for the NASTF Registry*.
 - 1.3.2.4. LSID account enrollment denials and LSID terminations may be appealed to the SRC through the registry appeals process as outlined in Attachment B – *Registry Denial and Dispute Resolution Appeal Process*.

ATTACHMENT A - CONTACT INFORMATION

Automotive Service Association	Associated Locksmiths of America	NASTF LSID Registry
Attn : President	Attn: Executive Director	Attn: NASTF Director
P.O. Box 929	3500 Easy Street	101 Blue Seal Drive, S.E.
Bedford, Texas 76095-0929	Dallas, Texas 75427	Suite 101
(817) 283-6205	(800) 532-2562	Leesburg, VA 20175
(800) 272-7467		(703) 669-6643
www.asashop.org	www.aloa.org	mhutchinson@asecert.org
Roles: <ul style="list-style-type: none"> • Funding • Industry Outreach 	Roles: <ul style="list-style-type: none"> • Funding • Registry Hosting • Registry Administration • Application Processing • Background Check • Record Maintenance • Industry Outreach 	Roles: <ul style="list-style-type: none"> • SDRM Administration • Dispute Resolution • Industry Awareness

ATTACHMENT B - REGISTRY DENIAL AND DISPUTE RESOLUTION APPEAL PROCESS

An applicant or LSID account holder will have the right to appeal to the **NASTF Security Review Committee (SRC)**: (a) a decision by the administrator of the NASTF LSID Registry to deny the applicant inclusion on the Registry, (b) a decision by the NASTF LSID Registry to suspend or terminate an LSID holder's rights with respect to the Registry, and (c) a denial by a Participating Automaker to permit access by the LSID account holder to Security Data on terms and conditions available to other LSID account holders.

RESPONSIBILITIES:

ALOA's responsibilities as the administrator and host of NASTF LSID Registry, include without limitation: (1) administering the application process, running background checks and making "go/no go" decisions on applicants based on criteria established by the NASTF VSC Policy Working Group. (2) acting as a clearinghouse for reports of improper use of the Registry, suspending accounts in cases of reported impropriety, passing evidence of said improprieties to the NASTF SRC for final disposition. ALOA is also responsible for canceling an LSID account if the SRC determines that reported impropriety is accurate.

NASTF Security Review Committee (SRC) is responsible for reviewing and making final decisions on rejected Registry applications that have been submitted for appeal.

The NASTF Security Review Committee (SRC)

The SRC will have seven (7) members. SRC members will be appointed by the NASTF Chairman. The SRC will include one (1) director from the NASTF Board of Directors, who will serve as chairman of the Committee, and six (6) committee members from outside the NASTF Board of Directors. The six members will be made up from two (2) members from the automotive service community, two (2) members from the locksmith community, and the other two (2) members to represent the automobile industry. Appointments to the SRC will be for a period of two (2) years. Committee members may be reappointed and there is no limit on the number of years an individual may serve in this capacity.

Registry Denial Dispute Resolution Appeal Process

- 1) The Registry Denial Dispute Resolution Appeal (DRA) process will allow an applicant to submit the SDRM Registry application and any additional information relevant to their circumstance to the SRC for review and final determination. The RDA process is outlined below:
- 2) Applicant has ten (10) business days to make written notification of an appeal from the date the notice of their application denial is received.

- 3) Appeal must be addressed to the NASTF Director at the address defined in attachment A.
- 4) Appeal must be made in writing and sent as certified mail through the United States post office.
- 5) Appeal must include permission for the SRC to access and review the same information that caused the denial for inclusion in the SDRM Registry.
- 6) Further, the appeal must acknowledge the determination of the SRC is final and the individual will not seek any remedy, legal or otherwise, beyond the scope of the RDA process. A denied applicant can not reapply for one (1) year from the date of receipt of the denied appeal decision.
- 7) The NASTF Director or designee, upon receipt of the appeal, will request the Registry Administrator to provide electronic copies of supporting documents used to deny Registry access and will confirm that the supporting documents and application are complete and sufficient to begin the appeal process.
- 8) Once determined complete, this information will be forwarded to the SRC opening the Dispute Resolution Appeal process.
- 9) The SRC will convene a meeting within ten (10) business days of receipt of supporting information from the NASTF Director or designee. The meeting can be by teleconference and will be recorded by the NASTF Director or designee.
- 10) The applicant will be notified of the SRC decision within fourteen (14) days from the date of the SRC appeal hearing. The notification will be sent to the applicant by certified mail through the United States post office.

Registry Suspension Dispute Resolution Appeal Process

The Dispute Resolution Appeal (DRA) process will allow a Primary LSID account holder to submit a rebuttal and appeal to the SRC in cases where an LSID account has been suspended. This is an opportunity for the LSID account holder to provide additional information to the SRC relevant to their circumstance. The DRA process is outlined below:

- 1) Per Section 1.2.12, when an LSID knows of another's violation of the terms and conditions, they are obligated to report said violation along with evidence of said violation to the NASTF Director. The NASTF Director, upon receipt of this evidence, shall contact the Registry Administrator to suspend the account. The Registry Administrator shall send a notice of suspension to the LSID account holder's email address of record.
- 2) The LSID account holder may appeal this suspension to the SRC by following steps 2 through 10 of the Registry Denial Dispute Resolution Appeal process.

ATTACHMENT C - Application Process for the NASTF Registry LSID ACCOUNT HOLDER - Application Process

- 1) Only original signed and notarized applications will be processed (see Attachment E – *Registry Application and User Agreement*).
- 2) The following documentation must be provided with the application:
 - a) A signed and notarized Registry Application and User Agreement (Attachment E – *Registry Application and User Agreement*),
 - b) Suitable proof of identity,
 - c) Proof of suitable fidelity bond and liability insurance that covers all employees who will use information acquired from the SDRM, as follows:
 - i) Liability insurance in the minimum amount of \$1,000,000 covering the business and all employees using information acquired through use of the Registry; and
 - ii) Fidelity or Employee Dishonesty Bond in the minimum amount of \$100,000 covering vehicle theft resulting from use of automotive security related service information acquired through use of the Registry or in lieu of the fidelity bond requirement, a Vicarious Liability rider to an existing insurance policy in the minimum amount of \$100,000.
 - d) Full dues payment including one time application fee.
- 3) Applicants will be notified via email that their application has been received and will be processed within 3 business days if all documentation is received.
- 4) Applicants will be notified within 3 business days if additional documentation or information is required before their application can be processed. Incomplete applications will be held for 90 days awaiting completion – after 90 days, incomplete applications will be discarded.
- 5) Applications which meet all requirements will be processed in within 72 business hours (in most cases).
- 6) Applicants will receive notification of the disposition of their application via US mail.

Background Check Procedures (Performed by Registry Administrator)

- 1) Search criteria will be entered into the secured website of the firm chosen to conduct the background check and archived as long as ALOA/ASA/NASTF are clients.
- 2) The following information will be used to conduct a basic internet background check:
 - a) First and last name, and middle initial (if provided)
 - b) Address including City, State and County

- c) Social Security Number
- 3) The internet background check requires:
 - a) Social security number trace – Via First Alert
 - i) The social security number is instantly validated.
 - ii) If invalid the applicant will be called to confirm information.
 - iii) If applicant is unable to provide a valid social security number the Adverse Action Process will be initiated.
 - b) Two level background check based on the social security number search
 - i) Minimal Due Diligence
 - (1) Searches the county records of the address provided.
 - (2) Lists all addresses associated to the social security number from 5 to 7 years old.
 - (3) Lists all “AKA’s” associated to the social security number from 5 to 7 years old.
 - ii) Maximum due Diligence
 - (1) Searches every county listed on the social security trace.
 - (2) Searches all “AKA’s” listed on the social security trace.
 - c) Criminal County Court search
 - i) search of all counties listed in social security trace
 - ii) the most current criminal activity posted in the county records
 - d) Verification of business license validity

Cause for Adverse Action

- 1) Registry applicants shall be rejected for:
 - a) Felony convictions and/or criminal convictions relating to any types of theft, larceny, auto theft or fraud.
 - b) Intentional deceit in the application process (i.e. providing inaccurate information with the intent of hiding background information)
 - c) Failure to provide suitable proof of bonding/insurance requirements
 - d) Failure to provide proof of a valid business and/or business location

- e) Failure to provide proof of a valid locksmith license, where required by state and/or local jurisdiction
- 2) Registry applicants may be rejected for felony convictions and/or criminal convictions related to crimes of violence or crimes committed with deadly weapons.

Adverse Action Process

- 1) Two letters will be sent to the applicant informing them of their right to dispute any adverse information returned through a background check.
- 2) First letter mailed within 5 business days of receipt of the report advising applicant of adverse information (an example letter is included in Attachment F – *Adverse Report Notification – 1st Letter*). The letter will include a complete copy of the report.
- 3) Second letter mailed within 5 business days of the first letters mailing date (an example letter is included in Attachment G – *Adverse Report Notification – Final Letter*). The letter will advise as to the final disposition if no other information is received to dispute the report.
- 4) All correspondence will be maintained with the original application.

Subordinate Enrollment Procedures (Performed by the LSID Business Owner or Primary LSID Account Holder)

- 1) It is a requirement that the Primary LSID account holder must perform a background check on subordinate account holder candidates. Background checks shall meet all Registry standards (noted above) and must be completed prior to adding an employee subordinate LSID account. This requirement is the responsibility of the Primary LSID Account Holder.
- 2) The employee background check shall include all items required of the Registry Administrator, see requirements outlined above - *Background Check Procedures (Performed by Administrator)*.
 - a) Acceptance criteria for subordinate LSID account holders is at the discretion of the business owner / Primary LSID account holder. As a minimum standard however, no individual shall be added as a subordinate LSID account holder if there is a record of any of the following:
 - i) Felony convictions and/or criminal convictions relating to any types of theft, larceny or auto theft
 - ii) Criminal convictions relating to fraud
- 3) The business owner shall follow the same (or similar) process, require the same application and supporting documentation as is required for a Primary LSID Account holder by the Registry
 - i) It is acceptable for the subordinate LSID account holder to be covered by the Primary LSID account holder (and/or business ID owner) liability insurance and fidelity bond.
 - ii) The Primary LSID account holder is required to maintain application and background check records for as long as an employee remains in the Registry.

- iii) The Primary LSID account holder shall run background checks on subordinate employees every three years.
- iv) The Primary LSID account holder must provide copies of the state trade licenses for the subordinate account holder candidates as a pre-condition to registration.
- b) The Primary LSID account holder attests to following these prescribed procedures every time the Registry is used by executing an electronic signature upon logging onto the Registry website.
- c) Failure to abide by this policy will result in termination of the business account.