



## What is the Secure Data Release Model - SDRM?

**SDRM** is a data exchange system conceived and designed cooperatively by automakers, the independent repair community, and the insurance and law enforcement communities; it allows the aftermarket to access security sensitive information related to automobiles i.e. key codes, PIN numbers, immobilizer reset information and similar types of information. SDRM allows access to security-related information while protecting the safety and security of consumers and the integrity of automobile security systems.

### Security Information Gaps that SDRM Addresses

Up until the development of SDRM, aftermarket service providers were unable to provide a limited number of services that required the use of security-related information. In some instances, information and/or special tools required to perform certain repairs like immobilizer reset functions, were protected by automaker security policies. Over the past several years, incidence of these types of repairs has increased due to proliferation of advanced security technology on large populations of mid-priced vehicles.

### How SDRM Resolves Security Information Gaps

Currently, technical information is publicly available via the web on a subscription basis. Until the advent of SDRM, security-related information was blocked from most parties except dealership personnel because there was no way to verify the security credentials of the requestor.

SDRM creates a Registry of automotive service/security professionals who have cleared a background check process. Automaker website subscribers who want to use security-related information can join the Registry. Security-related transactions are validated against the Registry and are fulfilled if the requestor's security credential is in good standing.

### Parties Responsible for SDRM and Registry

There are essentially four parties building and hosting SDRM and the Registry:

**NASTF**: responsible for industry outreach, systems development and dispute resolution. Through leadership from the NASTF Vehicle Security Committee (VSC), NASTF is responsible for bringing the parties together to identify and prioritize security information gaps and to help the Industry build and modify the systems necessary to close the gaps. The NASTF VSC has a standing Security Review Committee to manage disputes regarding enrollment in the Registry and access to security-related service information.

**Automakers**: responsible to host service information websites and/or call centers that serve as the portal to security-related service information. A complete list of automaker website URLs is available on the NASTF website at the [OEM Service Websites](#) link.

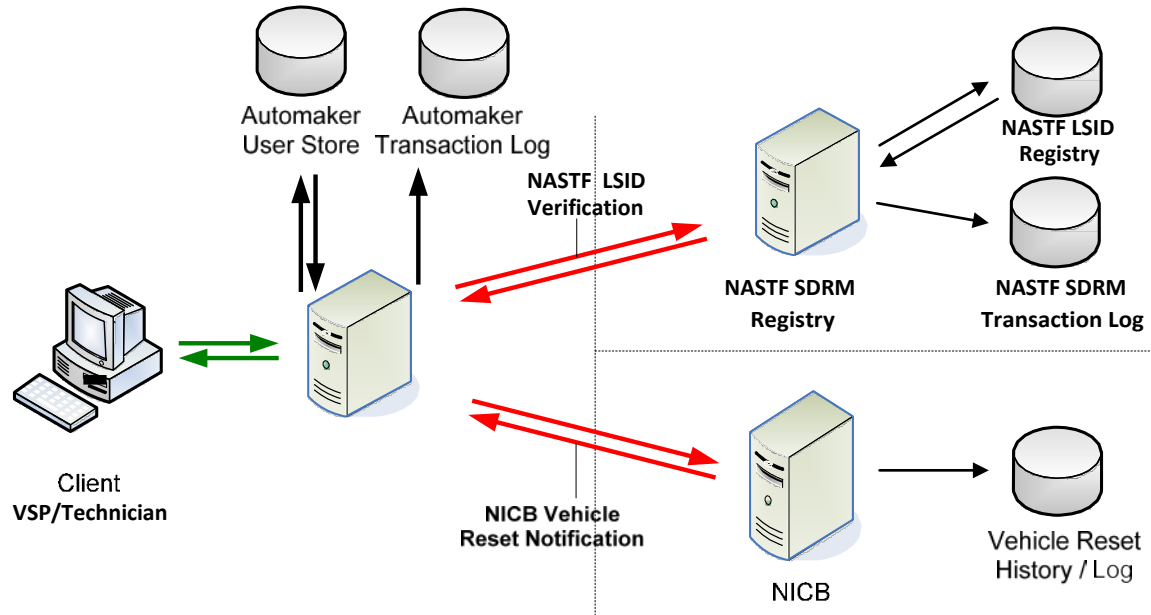
**ASA/ALOA**: responsible to host and administer the Registry website and database. These two aftermarket service trade associations provided the original funding for development and maintenance of the Registry. ASA currently is responsible for the application /background check process, user support and administration functions.

**NICB**: responsible to log transactions with automakers that involve security-related information. The National Insurance Crime Bureau protects consumers and automakers and also represents the insurance and law enforcement communities. NICB maintains transaction logs for all security-related information and provides forensic evidence to law enforcement to investigate automotive related crimes.

### How SDRM Works

The basic SDRM architecture is designed to provide system separation between automakers, NASTF and NICB through well-defined simple interfaces. Each automaker website uses standard web services to communicate with the NASTF SDRM and NICB.

Communication of required data and responses are done conforming to Industry specified web service protocols.



### Benefits of SDRM

The Secure Data Release Model (SDRM) provides safeguards to automakers and their customers to allow a change in the historic/customary practice of strict limitation of access to security-related service information, tools and components to the aftermarket.

SDRM provides:

- Consumer choice by ensuring that vehicle owners' can choose aftermarket service providers who have access to security related information, tools and components.
- Control of security-related information and tools by the owners of these resources -- the automaker and the consumer. No outside entity has access to, or control of the manufacturer's/consumer's data without strict security protocol and oversight.
- Improved indemnity (compared to many current practices) for automakers from legal actions resulting from the unauthorized use, misuse or illegal use of any security-related information.

SDRM ensures that responsibility for governance of independent repairers falls on the independent aftermarket service industry, not automakers. SDRM also meets insurance industry expectations for security with respect to release of security-related information.