



# SEQUITUR LABS, INC.

## Company Brief

### A New Way Forward

As mobile and other types of connected devices become increasingly central to enterprise computing, they bring with them opportunities for improvement as well as threats that can seriously compromise enterprise data, worker identity and corrupt key business applications.

Existing methods of securing and managing enterprise assets are rooted in decades old paradigms when the intrusion perimeter was a known and controlled element. With the emergence of smartphones, tablets and other devices that are not only mobile but always connected, the perimeter has vanished. Old approaches are less relevant. New thinking and approaches are needed to address the security requirements of a mobile enterprise. Sequitur is at the forefront of this thinking.

Sequitur Labs' vision is to create a platform and supporting technologies to better secure and manage connected devices of today and the future. It is for this reason that Sequitur has taken a leadership role in advancing the vision of *Trusted Mobility™*.

### What is Trusted Mobility™?

Trusted Mobility is an initiative to deliver tools, products and solutions to enterprises so that they can fully realize the potential of mobile computing with the assurance that corporate data assets, applications and employees are safe and secure. No single company can deliver on such a broad vision so a key imperative of the Trusted Mobility program is to build an ecosystem comprising enterprise ISVs, MNOs and device OEMs. Trusted Mobility starts with enabling enterprises to build secure applications and then manage those applications.

#### Secure Apps – The Bedrock of Trusted Mobility

Trusted Mobility begins with first building secure mobile apps. Sequitur has partnered with Trustonic to make this a reality. Trustonic provides a Trusted Execution Environment (TEE) on mobile devices allowing enterprises to leverage the hardware root of trust available in hundreds of millions of devices in their applications. Sequitur's *SeqrTRUST™* product is a library and a suite of trusted services that allow enterprises to rapidly build trusted applications without having to learn the intricacies of developing for the TEE.

In-house enterprise developers, enterprise ISVs and custom app developers benefit from drastically reduced time to market for developing secure apps.

#### Responsive App and Device Management

Developing secure apps is only the first step. As any IT manager worth his or her salt knows, the cost of managing apps through their lifecycle combined with the effort required to manage mobile devices is much greater than the initial cost of developing the app itself. That cost is often driven by outdated policy models that are largely static in their enforcement. Current policy models take away device functionality resulting in IT managers having to constantly intervene and push new policies that return functionality to users.

Sequitur's approach is unique. Sequitur is pioneering an entirely new policy enforcement paradigm called *Event Centric Authorization™* (ECA). ECA based policies are dynamically enforced taking into account the discreet devices events, application contexts and user roles – in real time. This intelligent enforcement of policies means that IT personnel do not need to constantly intervene to push new policies to devices in order to return functionality to users.

More importantly, the policies themselves are routed through the TEE ensuring that they have not been tampered with.

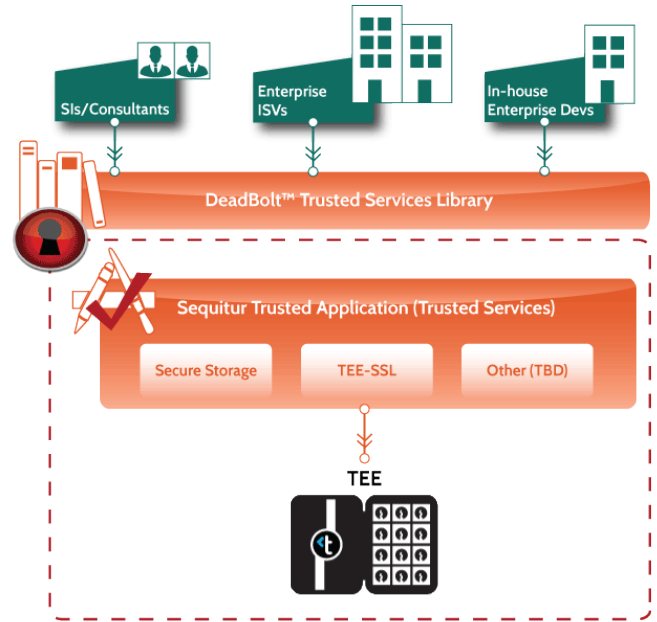
## SeqrTRUST™ – Secure Enterprise Application Development

SeqrTRUST is a suite of trusted services that allow developers an easy path to developing applications for the Trustonic TEE. These trusted services include:

- Secure File System
- Secure Network Communications
- More to come.....

Developers access the above services using the SeqrTRUST library when developing their applications. Using SeqrTRUST developers can implement greater degrees of security in their apps with improved:

- Transactional integrity
- Device authentication
- ID protection
- Data protection (Data-at-Rest)
- Application attestation
- More secure communication (Data-in-Transit)



SeqrTRUST dramatically reduces the time taken to developing secure TEE based applications since developers need not learn the intricacies of writing apps for the TEE.

## SeqrEMP™ – Your Business, Your Rules

SeqrEMP implements a pioneering approach – Event Centric Authorization (ECA) enabling dynamic policy enforcement and robust, fine grained policy authoring. With SeqrEMP, enterprises, carriers and managed service providers can use a single platform to customize device and application management policies for multiple organizations and customers. Policies are responsive to device and user contexts, making device and application functionality available when needed.

SeqrEMP implements:

- Unique hierarchical policy authoring model
- Geo-location based policy enforcement
- Programming language based policy authoring
- Malware/root access prevention
- Authorized/Unauthorized app listing and conditional control of applications
- Integration with LDAP/AD for rapid user enrollment

	Security Model	Authoring	Deployment	Administration
<b>Summary highlights</b>	<ul style="list-style-type: none"> <li>▪ Event driven</li> <li>▪ Context aware</li> <li>▪ Real time</li> </ul>	<ul style="list-style-type: none"> <li>▪ Programmable</li> <li>▪ Flexible</li> </ul>	<ul style="list-style-type: none"> <li>▪ Flexible policy server deployment</li> <li>▪ Policy server Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ Web based admin console</li> <li>▪ User enrollment</li> <li>▪ Hierarchical</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>▪ Dynamic, conditional policy enforcement</li> <li>▪ Maintains user productivity and experience</li> </ul>	<ul style="list-style-type: none"> <li>▪ Fine grained policies</li> <li>▪ Mapped to user roles</li> <li>▪ Customizable for industries &gt; business units &gt; organizations</li> </ul>	<ul style="list-style-type: none"> <li>▪ Better customer choices</li> <li>▪ Device driven</li> </ul>	<ul style="list-style-type: none"> <li>▪ Empower the eco-system</li> </ul>

This enables customers to:

- Implement far more effective BYOD programs
- Reduce the need for constant IT intervention to push new policies
- Customize policies to reflect their precise business needs
- Deploy a scalable platform capable of supporting millions of devices
- Re-program policies and readily adapt to changing business and IT needs and requirements imposed by new devices

### CONTACT

JENNIFER MULTARI  
 Marketing Communications Manager  
 jennifer.multari@sequrlabs.com  
 www.sequiturlabs.com