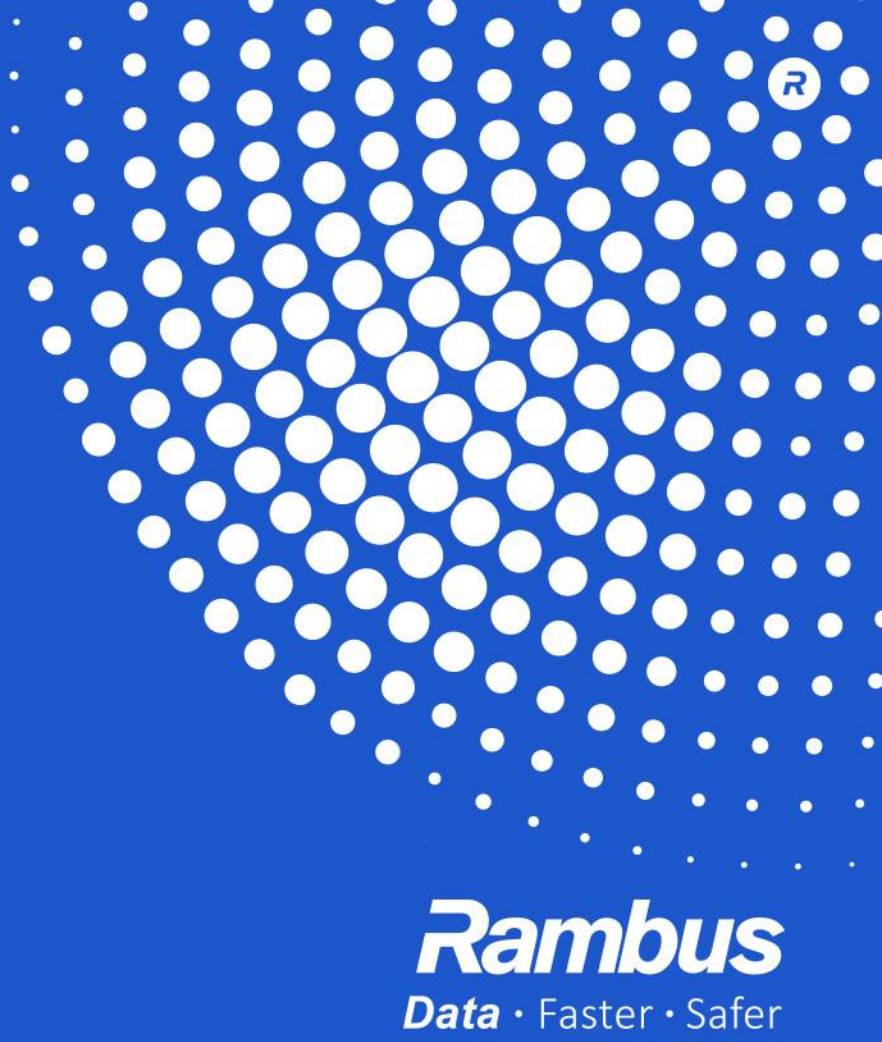
Security Issues in the Supply Chain

Helena Handschuh

08/28/2018



Semiconductor Manufacturing Challenges

	Lack of Trust in Supply Chain	High Cost of Multiple SKUs
		
Challenges	• Untrusted production environments • Overbuilding/overproduction • Reverse engineering/cloning/IP Theft • Grey market chips/ knock offs • Limited production visibility • Costly audits	• Multiple SKUs/single die increase production and testing costs • Forecasting and production forecasting is uncertain • Feature settings irreversible
Impact	• Lost revenue • Liability • Safety issues • ASP Erosion • Company / Product reputation • Additional support burden	• Overbuild: inventory spoilage • Underbuild: missed market opportunities and perishable demand • Complex and costly supply chain logistics • Costly inventory management

Requirements/solutions for better supply chain security

- Secure device configuration
- On-chip access control and rights management
- Identity assurance and traceability
- Attestation (what about anonymity?)
- Certificates and revocation, TTPs, CRLs?
- Secure distributed key management and KMS
- Secure Personalization and key injection/on-board key gen
- Chicken and egg problem?
- Secure facilities; Tester security?
- Multiple stage device lifecycle management
- Secure Part #/inventory management
- Secure Debug and RMA
- Secure Audit/logs/data management

- How does this work for Secure Enclaves?