

Table of Contents

1. The Reference Architecture at a Glance	
2. Why AI Factories Are Different	
3. Regulatory and Sovereignty Considerations	
4. The Seven Security Pillars	
5. The Seven Policy Enforcement Points	
6. Data Flow Walkthrough	
7. Building the Identity Pillar	
8. Building the Perimeter Pillar	
9. Building the Model Protection Pillar	
10. Building the Compute Pillar	
11. Building the Data Protection Pillar	
12. Building the Secure AI Operations Pillar	
13. Identity Enforcement Point	
14. Perimeter Enforcement Point	
15. Model Plane Enforcement Point	
16. East–West Enforcement on the DPU	
17. Micro-segmentation & Runtime Enforcement Point	
18. Data Protection Enforcement Point	
19. Observability & Response Enforcement Point	
20. Building a Sovereign AI Factory	
Conclusion	
Glossary	
Appendices A–J	
Index	