PUBLIC TECHNICAL REVIEW PACKAGE

FHE/ZK/VFHE Security Research

A public review document for encrypted-computation security research that supports AI system development without exposing private construction details.

Core in one sentence FHE/ZK/VFHE research gives the AI system a privacy and verification foundation.	**Most important point** The security track makes the portfolio stronger because trust, privacy, and reviewability are part of the base layer.

FHE/ZK	VFHE	Clear	AI stack
security foundation	verifiable encrypted-computation track	public presentation readiness	security-to-AI bridge

What this PDF is meant to prove

- Security research is the first foundation of the AI development story.
- FHE/ZK/VFHE direction creates public language for privacy, verification, and protected computation.
- The role is presented carefully: component value is public, protected internals stay private.
- The track connects to Web AI infrastructure through trust boundaries, validation paths, and review language.

Purpose Explain why encrypted-computation research matters for a developed AI infrastructure portfolio.	**Difference** Present privacy and verification direction as a foundation layer rather than a side topic.
Advantage Makes the AI system story stronger because security is part of the architecture from the start.	**Boundary** No protected construction details are included in the public document.

Inside this document

Page	Section	What the reviewer should learn
2	1. Development Role	This track gives the portfolio a security-first foundation.
3	2. Security Track Comparison	This table describes the difference from existing roles at a public architecture level.
4	3. Public Component Register	The register gives presentation-ready language for each part of the security track.
5	4. Advantages and Constraints	This track has strong positioning value when it is presented with clean boundaries.
6	5. Readiness and Evidence Plan	The goal is to make the security track easy to understand for a technical audience and a non-specialist audience.
Guide	Plain-English Presenter Guide	Simple public explanation and Q&A; for non-specialist review.
Final	Public Boundary and Presentation Notes	How to explain the work strongly while keeping private internals excluded.

Fast presentation line

Formysec develops AI security infrastructure by connecting security modules, custom execution foundations, LLM acceleration, and Web AI system development into one reviewable portfolio.

1. Development Role

This track gives the portfolio a security-first foundation. Instead of presenting AI work as only model behavior, it frames the lab as developing infrastructure where privacy, validation, and protected computation are part of the system.

- FHE direction: privacy-preserving computation language and protected-state direction.
- ZK direction: verification-oriented review language without exposing private internals.
- VFHE direction: verifiable encrypted-computation research track for stronger review posture.
- AI connection: security research supports trusted AI system development.

Before Security, model execution, and web service work can look disconnected.	**After** The portfolio shows security research as the base layer for AI infrastructure.
Reader benefit A non-specialist can understand the role without seeing protected internals.	**Technical benefit** The stack can be discussed by trust boundary, validation role, and system connection.

Presenter Notes

Plain-English angle This page explains 1. development role in simple terms: what was developed, why it matters, and how it should be reviewed.	**Technical angle** Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.
Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	1. Development Role describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

2. Security Track Comparison

This table describes the difference from existing roles at a public architecture level.

Security area	Typical existing role	Formysec public framing	Advantage and limit
FHE direction	Privacy computation treated as a separate research topic.	Presented as part of the AI system foundation.	Advantage: stronger security story. Limit: public package stays architecture-level.
ZK direction	Verification handled as a separate compliance or result-review layer.	Presented as review direction connected to module and validator paths.	Advantage: clearer review story. Limit: private internals are excluded.
VFHE direction	Encrypted computation and verification can be discussed separately.	Presented as a combined research direction for verifiable encrypted computation.	Advantage: higher-level trust story. Limit: more external records would strengthen it.
AI infrastructure bridge	AI systems may be presented without a security foundation.	Security track becomes the foundation for developed AI systems.	Advantage: professional lab positioning. Limit: public evidence must stay scoped.

Presenter Notes

Plain-English angle This page explains 2. security track comparison in simple terms: what was developed, why it matters, and how it should be reviewed.	**Technical angle** Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.
Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	2. Security Track Comparison describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

3. Public Component Register

The register gives presentation-ready language for each part of the security track.

Item	What it contributes	How to present it	What not to expose
FHE research direction	Privacy-preserving computation foundation.	A base layer for protected computation in AI infrastructure.	No protected construction detail.
ZK research direction	Verification and review framing.	A result-review direction connected to validator-compatible records.	No sensitive internal method.
VFHE track	Verifiable encrypted-computation direction.	A stronger bridge between protected computation and reviewability.	No private technical internals.
Security-to-AI bridge	Connects the security layer to AI development.	Security is part of the developed AI system, not an add-on.	No overstatement beyond public records.

Presenter Notes

Plain-English angle This page explains 3. public component register in simple terms: what was developed, why it matters, and how it should be reviewed.	**Technical angle** Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.
Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	3. Public Component Register describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

4. Advantages and Constraints

This track has strong positioning value when it is presented with clean boundaries.

Advantage 1 Raises the portfolio from web AI presentation to AI security infrastructure development.	**Advantage 2** Makes privacy, validation, and reviewability part of the system foundation.
Advantage 3 Supports a research-lab identity across modules and AI infrastructure.	**Constraint** The public version must stay at role, evidence, and boundary level.

- Best public phrasing: FHE/ZK/VFHE security research supports the developed AI system stack.
- Avoid public deep detail; focus on what the track enables and how it connects to modules.
- State that longer external review records are a strengthening step, not a missing identity.
- Keep performance statements attached to measured modules rather than the abstract security track.

Presenter Notes

Plain-English angle This page explains 4. advantages and constraints in simple terms: what was developed, why it matters, and how it should be reviewed.	**Technical angle** Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.
Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	4. Advantages and Constraints describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

5. Readiness and Evidence Plan

The goal is to make the security track easy to understand for a technical audience and a non-specialist audience.

Evidence area	Current state	Why it matters	Next strengthening step
Public explanation	Clear website and PDF language.	Makes the track understandable to reviewers.	Add a dated research-note index.
Component bridge	Security track connected to RMEP, validator, and AI layers.	Shows system thinking.	Add more architecture diagrams.
Performance linkage	Performance records sit mainly in RMEP and LLM PDFs.	Keeps abstract security statements careful.	Add workload labels where records connect.
Boundary control	Protected internals excluded.	Keeps the public package credible.	Maintain a release checklist before every upload.

Presenter Notes

Plain-English angle This page explains 5. readiness and evidence plan in simple terms: what was developed, why it matters, and how it should be reviewed.	**Technical angle** Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.
Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	5. Readiness and Evidence Plan describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

Plain-English Presenter Guide

This page gives the short explanation before a deeper technical review. It is designed for non-specialists and for fast presentation flow.

Review step	What it explains	What evidence follows	Do not mix with
Thesis	Formysec develops AI security infrastructure from modules to Web AI.	Master portfolio and topology.	Internal benchmark details.
Enterprise lens	A small research lab produced a broad, reviewable security and AI infrastructure package.	Enterprise review table and evidence ledger.	Universal deployment promises.
Architecture	Security base, RMEP modules, foundation, LLM acceleration, and Web AI delivery.	Stack map and layer descriptions.	Baseline comparison.
External comparison	Comparison evidence for module role, validation workflow, consistency, and LLM infrastructure.	Security-module comparison, validator-workflow comparison, LLM-infrastructure comparison, and implementation-check summaries.	General overview language.
Track details	Each field gets its own role, value, evidence style, and boundary.	Field PDFs and component pages.	One overloaded table.
Comparison	What the work may replace, complement, or improve.	Baseline comparison table.	Private construction details.
Evidence and scope	What is public, what was checked, and what remains private.	Evidence PDF, public scans, live checks.	Sensitive internal design notes.

Reviewer Q&A;

Reviewer question	Short answer	Evidence to point at	Boundary
What is the portfolio?	A technical review package for AI security infrastructure built from modules, foundation work, LLM acceleration, and Web AI.	Portfolio structure page and master PDF.	Private internals excluded.
Why should a company care?	It shows a lean lab with broad execution: security modules, AI acceleration, Web AI delivery, protocol builds, and evidence control.	Enterprise review lens, evidence ledger, and live site.	Not a final product approval statement.
Where is the evidence?	It is organized in the external comparison register so evidence does not get mixed with overview text.	External comparison table and evidence PDF.	Records are condition-labeled.
How is RMEP framed?	RMEP is structure-first module development; execution paths carry the structure rather than replace it.	RMEP PDF and result register.	Not a final-standard statement.
Is this ordinary model access?	No. The public position is development of acceleration code, routing, API behavior, Web AI layer, and evidence packaging.	LLM acceleration PDF and Web AI section.	Performance varies by workload and baseline.

Presenter Notes

Plain-English angle
This page explains plain-english presenter guide in simple terms: what was developed, why it matters, and how it should be reviewed.

Technical angle
Focus on component role, existing-role comparison, advantage, limit, evidence type, and public boundary.

Strong answer Start with the developed part, compare it with a familiar external role, then state the boundary so the statement stays credible.	**Review caution** Keep protected construction details outside the public explanation and point back to the published evidence package.

Review Questions

Reviewer question	Public answer
What was developed?	Plain-English Presenter Guide describes a developed part of the Formysec stack and connects it to the larger AI security infrastructure story.
How is it different?	The page compares the developed role against an existing technical role, then explains the advantage and the current evidence.
What is the boundary?	The public answer stays with component role, external comparison, readiness state, and public evidence while protected construction details remain excluded.

Public Boundary and Presentation Notes

This final page keeps the package strong and objective during presentation.

- The document presents component roles, external comparison labels, evidence scope, and readiness state.
- Private technical internals, protected implementation details, and sensitive construction notes stay outside this public package.
- Performance evidence remains tied to workload, environment, review method, and external comparison baseline.
- The language is intentionally objective: strong enough for a technical presentation, careful enough for review.

Recommended speaking frame

- Say that Formysec develops AI security infrastructure across security modules, execution foundations, LLM acceleration, and Web AI system layers.
- Say records are review records with stated boundaries, not universal production guarantees.
- Say that the portfolio is designed to be understandable without exposing protected internal construction.
- When asked for deeper internals, redirect to public component roles, comparison evidence, and review roadmap.